(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年2 月22 日 (22.02.2001)

PCT

(10) 国際公開番号
WO 01/13293 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP00/05439

(22) 国際出願日: 2000 年8 月14 日 (14.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/228154 1999 年8 月12 日 (12.08.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 中西良明 (NAKANISHI, Yoshiaki) [JP/JP]; 〒166-0014 東京都杉並区松ノ木2-4-10-305 Tokyo (JP). 高山 久 (TAKAYAMA, Hisashi) [JP/JP]; 〒156-0043 東京都世田谷区松原5-6-12 Tokyo (JP). 松瀬哲朗 (MATSUSE, Tetsuo) [JP/JP]; 〒565-0853 大阪府吹田市春日2-6-3-109 Osaka (JP).

(74) 代理人: 弁理士 蔵合正博, 外(ZOGO, Masahiro et al.); 〒102-0083 東京都千代田区麹町5丁目7番地 秀和紀尾井町TBRビル Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

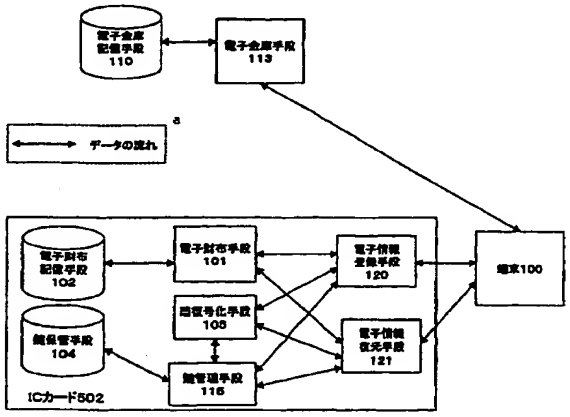
(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: ELECTRONIC INFORMATION BACKUP SYSTEM

(54) 発明の名称: 電子情報バックアップシステム



(57) Abstract: An electronic information backup system for safely back up electronic value information about electronic money and electronic ticket through communication in a server so as to exclude unauthorized actions when backup and restoring are performed and for restoring the electronic value information from the backup in case of emergency such as loss of key information. In this system, electronic value information is encrypted, the encrypted electronic value information is registered in an electronic safe server, and the user receives the registration, presents the registration to the server to receive the encrypted electronic value information, and decrypts the electronic value information with decrypting key data. The decrypting key can be kept in another server. The electronic value information and the decrypting key can be kept separately in different servers. It is possible to keep the sequence of number of the cryptogram to serve as the basic the decrypting key in the server, and to generate a decrypting key according to a decrypting key generation algorithm on the terminal side. In case of loss of the decrypting key, the possessor certificate information is verified and then the user can receive the decrypting key from the server.

[続葉有]

WO 01/13293 A1

(57) 要約:

通信を介してサーバ上に電子マネーや電子チケット等の電子価値情報を安全にバックアップし、バックアップと復元の際に不正行為を排除し、鍵情報消失などの緊急時に電子価値情報をバックアップから復元する電子情報バックアップシステムを提供する。このシステムでは、電子価値情報を暗号化して電子金庫サーバ上に登録してその登録証を受け取り、後に、登録証をサーバに提示して暗号化電子価値情報を受け取り、データ化された復号鍵で復号する。復号鍵は別のサーバに預けてもよい。また、電子価値情報及び復号鍵を分割して、別々のサーバに預けてもよい。また、復号鍵の元となる暗号の数列をサーバに預け、端末側ではそれを復号鍵生成アルゴリズムを用いて復号鍵に生成してもよい。復号鍵を紛失した場合は、所有者認証情報を検証した後、サーバから復号鍵を受け取ることができる。

明　細　書

電子情報バックアップシステム

技術分野

本発明は、コンピュータと情報通信を用いたバックアップシステム、特に電子現金や電子チケットといった電子価値情報のバックアップと復元を行なうシステムに関するものである。

背景技術

電子現金や電子チケットなどの金銭もしくは金銭的価値のある情報を、電子的な形式で表現し利用する技術が一般的となってきている。電子現金や電子チケットなどの電子的に表現された価値情報を、以下、電子価値情報とする。

電子価値情報の実現方法の一つとして、遠隔地のサーバ上で電子価値情報を置き、その所有者は認証情報のみを持ち、利用時にサーバと通信するようにする方法がある。前記の方法では、認証の安全性を確保する事によって安全な取り引きを実現できるが、ネットワークに接続できる状態でなければ電子価値情報を使用できないという問題や、ネットワークへの問い合わせが使用の度に発生するため、高速な反応を要求する状況には適用しにくいという問題がある。

そのため、ネットワークと独立した状態でも電子価値情報を利用することが出来るように、電子価値所有者の持つICカード、携帯電話、携帯端末などのデバイス上に電子価値情報そのものを保持するようにする技術も存在する。ただしこの場合、デバイスの破損や紛失によって電子価値情報が消失してしまう危険性を持っている。

上記の電子価値情報を含む電子情報の破壊という問題からの回復を実現するため、従来いくつかの技術が考案されている。以下にその例を示す。

第一の従来技術として、特開平１０－１３３９２５号公報に示される技術では、暗号化したメールを用いることで、ファイヤーウォール内から外のバックアップサーバに対してデータのバックアップを行う。ただしこの技術では、鍵の紛失や破損時に暗号化したデータからの復元方法については考慮されていない。

第二の従来技術として、米国特許５、７７８、３９５に示される技術では、ネ

ットワークに繋がったノード(コンピュータ)のファイルを別のノード上のサーバに圧縮や暗号化を行ってバックアップする。ただしこの技術でも、第一の従来技術と同様に鍵の紛失や破損時のことが考慮されていない。

上述のように、従来技術は、暗号によって秘匿した状態で電子情報のバックアップと復元を行うものであった。しかし、従来技術では、暗号に用いた鍵情報が消失した場合に暗号化されたバックアップ情報を復元することについて考慮されていないため、鍵情報も含めた電子情報を格納したデバイスの紛失や破壊などに対処できないという問題がある。

また、上記の問題に対応するために暗号の復号に用いる鍵を単純にバックアップしたとしても、鍵を預けたサーバと暗号化した電子価値情報を預けたサーバの両者が共謀するなど、鍵のバックアップ管理の信頼性を損なうような不正行為に対しても対処しなければならない。

発明の開示

本発明の目的は、通信を介してサーバ上に電子価値情報を安全にバックアップすることと、バックアップと復元の際に不正行為を排除することと、鍵情報消失などの緊急時に電子価値情報をバックアップから復元することを可能とする電子情報バックアップシステムを提供することにある。

本発明によれば、電子価値情報を暗号化して電子金庫サーバ上に登録してその登録証を受け取り、次に、登録証をサーバに提示して暗号化電子価値情報を受け取り、データ化された復号鍵で復号するシステムが提供される。復号鍵はユーザが持っていてもよいし、サーバに預けてもよく、さらに、別のサーバに預けてもよい。また、電子価値情報を分割し、さらには復号鍵をも分割し、両者を一体に或いは部分的に一体にサーバに預けるか、またはまったく別々のサーバに預けてもよい。また、復号鍵の元となる暗号の数列をサーバに預け、端末側ではそれを復号鍵生成アルゴリズムを用いて復号鍵に生成してもよい。復号鍵を紛失した場合は、所有者認証情報を検証して検証が成功すれば、サーバから復号鍵を受け取ることができる。

図面の簡単な説明

第１図は、本発明の実施の形態１における電子情報バックアップシステムの構成図である。

第２図は、本発明の実施の形態１における電子価値情報とダイジェスト情報と登録証の模式図である。

第３図は、本発明の実施の形態１における電子財布手段上での電子価値情報と登録証の管理方法を示す模式図である。

第４図は、本発明の実施の形態１における電子金庫記憶手段での情報保管方法を示す模式図である。

第５図は、本発明の実施の形態２における電子情報バックアップシステムの構成図である。

第６図は、本発明の実施の形態２における登録電子価値情報と登録証の模式図である。

第７図は、本発明の実施の形態２における鍵保管手段上での暗号鍵と復号鍵の保管方法を示す模式図である。

第８図は、本発明の実施の形態２における鍵管理記憶手段上の鍵情報の管理方法を示す模式図である。

第９図は、本発明の実施の形態２における電子金庫記憶手段での情報保管方法を示す模式図である。

第１０図は、本発明の実施の形態３における電子情報バックアップシステムの構成図である。

第１１図は、本発明の実施の形態４における電子情報バックアップシステムの構成図である。

第１２図は、本発明の実施の形態５における電子情報バックアップシステムの構成図である。

第１３図は、本発明の実施の形態６における電子情報バックアップシステムの構成図である。

第１４図は、本発明の実施の形態７における電子情報バックアップシステムの構成図である。

第１５図は、本発明の実施の形態８における電子情報バックアップシステムの構成図である。

第１６図は、本発明の実施の形態９における電子情報バックアップシステムの構成図である。

第１７図は、本発明の実施の形態１０における電子情報バックアップシステムの構成図である。

第１８図は、本発明の実施の形態１１における電子情報バックアップシステムの構成図である。

第１９図は、本発明の実施の形態１１における電子財布記憶手段上の電子価値情報群を示す模式図である。

第２０図は、本発明の実施の形態１１における電子財布記憶手段上の電子価値情報群を示す模式図である。

第２１図は、本発明の実施の形態１２における電子情報バックアップシステムの構成図である。

発明の好ましい実施の態様

本発明は、第１に、ローカルの電子価値情報を電子金庫サーバ上に登録してその登録証を受け取り、その登録証を電子金庫サーバに提示することにより、対応する電子価値情報を取得できるようにしたものである。これにより、ローカルの電子価値情報が破損した場合でも電子価値情報を復元することが可能になる。

本発明は、第２に、ローカルの電子価値情報を暗号化して電子金庫サーバ上にバックアップする。これにより、電子価値情報を電子金庫サーバに隠蔽した状態でバックアップすることができ、ローカルの電子価値情報が破損した場合でも電子価値情報を復元することが可能になる。

本発明は、第３に、暗号化した電子価値情報を復号化するための復号鍵を異なる電子金庫サーバにバックアップする。これにより、電子価値情報をより安全に保管することが可能になる。

本発明は、第４に、電子価値情報を分割してそれぞれを異なる電子金庫サーバにバックアップする。これにより、バックアップ時の全通信路の傍受や、全電子

金庫サーバへの不正侵入を行うなど、不正に前記復号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第5に、複数の電子価値情報を結合して暗号化し、電子金庫サーバにバックアップし、電子金庫サーバから取得した時に結合を分離して電子価値情報を復元する。これにより、バックアップ時の全通信路の傍受や、全電子金庫サーバへの不正侵入を行うなど、不正に前記暗号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第6に、復号鍵を分割して、一方の分割鍵を電子価値情報とともに一方の電子金庫サーバにバックアップし、他方の分割鍵を他方の電子金庫サーバにバックアップする。これにより、バックアップ時の全通信路の傍受や、全電子金庫サーバへの不正侵入を行うなど、不正に前記暗号鍵を取得する困難度が高くなる。また、それぞれの電子金庫サーバの独立性が高ければ、電子金庫サーバ管理者の共謀による復号鍵の不正な復元が行われる可能性を低くすることができる。

本発明は、第7に、復号鍵を数学的に生成するために用いる元の暗号種（たね）情報を電子金庫サーバにバックアップし、復元時に暗号種情報を電子金庫サーバから受け取り、暗号種情報から復号鍵生成アルゴリズムを通して復号鍵を生成する。これにより、電子価値情報のみならず、復号鍵の安全性が極めて高くなる。

本発明は、第8に、所有者情報と認証情報とを照合して一致した場合に電子金庫サーバから電子価値情報を取得可能とする。これにより、復号鍵を紛失したり、端末が破壊されてデータが取り出すことができない場合でも、電子金庫サーバから復号鍵を取得して電子価値情報を復元することができる。

本発明は、第9に、予め設定したバックアップ条件に従って電子価値情報を選択する。これにより、バックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうので、ユーザの負担を軽くすることができ、端末のメモリ容量や通信にかかるコスト(時間、費

用)を抑えることができる。

本発明は、第１０に、安全のために電子価値情報と復号鍵を別の電子金庫サーバに預けた場合に、認証によって正当な情報保持者と認定された場合には、電子金庫サーバ同士が通信を行なって、電子価値情報と復号鍵とを合わせて送り返してくるので、復号鍵を紛失した時や端末が破壊されてデータを取り出すことができない時でも、電子価値情報を復元することができる。また、電子価値情報を直ぐに利用しない場合は、新たな暗号鍵を用いて電子価値情報を暗号化し、それを一方の電子金庫サーバに送るとともに、復号鍵を他方の電子金庫サーバに送ることにより、従前の状態に戻すことができる。

実施例

以下、図面を用いて本発明の実施例について説明する。なお、本発明はこれらの実施例に何ら限定されるものではなく、その要旨を逸脱しない範囲に置いて種々の態様で実施し得る。各図は図１、図２・・・のように表示する。

実施例１

図１、図２、図３、図４を用いて、本発明の請求項１、２、３に係る第１の実施例について説明する。図１は本実施例１が示す電子情報バックアップシステムの一例を示した構成図である。本システムは基本的に有線または無線の通信路によって結ばれたコンピュータ装置と、それに接続された外部拡張機器およびそれらの上で動作するソフトウェアで構成されるものとする。ここでいうコンピュータ装置とは、ソフトウエアプログラムに従って動作する中央演算装置を備えた機器の総称を意味するものとする。

本実施例１では、電子財布手段１０１および電子財布記憶手段１０２および電子情報登録手段１０６および電子情報復元手段１０７は、ＩＣカード５０１内に構成される。端末１００は、ＩＣカードリーダ・ライタを備えた携帯電話端末であり、ＩＣカード５０１内に構成された電子情報登録手段１０６および電子情報復元手段１０７と通信することができる。端末１００とサーバである電子金庫手段１０３は、無線によって通信する。なお、端末１００は、ＩＣカードリーダを備えたパーソナルコンピュータ、またはセットトップボックス、または携帯型コ

ンピュータであっても良い。なお、端末１００と電子金庫手段１０３の間の通信は、有線通信であってもよい。なお、ＩＣカード５０１と同等の機能を持つものを、端末１００内に内蔵して構成してもよい。

電子財布手段１０１および電子情報登録手段１０６および電子情報復元手段１０７は、ソフトウェアと、このソフトウェア格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって実現される。また、電子財布手段１０１は、電子財布記憶手段１０２の内容の参照と変更を行なうことができる。電子財布記憶手段１０２は、ＥＥＰＲＯＭなどの書き換え可能なメモリによって実現される。

電子価値情報とは電子現金や電子チケット、電子クーポンなどを表す電子情報であり、登録証とは前記電子価値情報を電子金庫手段１０３に登録したさいに発行される前記電子価値情報の控えを表す電子情報である。図３に電子財布記憶手段１０２での電子価値情報と登録証の管理方法を示す。電子財布手段１０１は、電子財布記憶手段１０２上にインデックス８５１を置く。前記インデックス８５１は、電子財布記憶手段１０２上に格納された情報に対するポインタと前記情報のサイズとポインタの先の情報の種別を表す記号の組をまとめたものである。これにより、電子財布手段１０１は次に示す機能を実現できる。

電子財布手段１０１は、電子財布記憶手段１０２中のインデックス８５１を参照してポインタとサイズを取得し、取得したポインタとサイズを用いて電子価値情報または登録証を取り出すことができる。電子財布手段１０１は、電子財布記憶手段１０２中のインデックス８５１を参照してすべてのポインタとサイズを取得し、それを用いて、すべての電子価値情報と登録証のタイトル情報を取得する。前記のポインタとサイズタイトルを用いて、全保管情報のリストを作成することができる。また、特定の条件に合致するポインタとサイズを取得することで、条件に合致する情報のリスト（例えば登録証のリストや有効期限完了まで残り一週間以内の情報のリストなど）を作成することもできる。

また、電子財布手段１０１は、電子財布記憶手段１０２中の空き領域に電子価値情報または登録証を書き込み、それに対応する種別とポインタとサイズの組の

エントリをインデックス８５１に追加することで、電子財布記憶手段１０２に電子価値情報または登録証を保管することができる。その逆に、インデックス８５１中に示されたポインタとサイズを参照して、前記ポインタとサイズが指す領域を消去し、前記ポインタとサイズに対応したエントリをインデックス８５１から削除することで、電子財布記憶手段１０２から電子価値情報または登録証を削除することができる。また、新規登録と削除を組み合わせることで、電子価値情報または登録証の情報を修正することができる。なお、上記の仕組みは、ＩＣカード５０１上のオペレーティングシステム（ＯＳ）が持つファイルシステムの機能を用いて実現しても良い。

電子情報登録手段１０６は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。なお、電子情報登録手段１０６と電子財布手段１０１はＯＳとＣＰＵを共有してもよい。電子情報登録手段１０６は、電子財布手段１０１から電子価値情報を取得することと、登録証を電子財布手段１０１に登録することを行う。また、電子情報登録手段１０６は、電子財布手段１０１から電子価値情報の一覧を取得する。

電子情報復元手段１０７は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。なお、電子情報復元手段１０７と電子財布手段１０１はＯＳとＣＰＵを共有してもよい。電子情報復元手段１０７は、電子財布手段１０１から登録証を取得することと、電子価値情報を電子財布手段１０１に登録することを行う。また、電子情報復元手段１０７は、電子財布手段１０１から登録証の一覧を取得する。

電子金庫手段１０３は、ワークステーションまたはパーソナルコンピュータなどのコンピュータ装置と、前記コンピュータシステム上で動作するソフトウェアから構成される。電子金庫手段１０３は、電子金庫記憶手段１１０の内容の参照と変更を行なうことができる。電子金庫記憶手段１１０は、電子金庫手段１０３が内容の参照と変更を行なうことができる記憶装置であり、ハードディスクなど

で実現される。電子金庫記憶手段１１０上には、前記コンピュータシステムのＯＳが管理するファイルシステムが構築されている。

図２（ａ）は電子価値情報の一例として電子価値情報２０１を示す。電子金庫手段１０３が電子価値情報２０１の登録要求を受けた場合、図２（ｃ）に示す登録証３０１を電子価値情報２０１を用いて生成する。登録証３０１を生成する処理の流れを以下に説明する。

電子金庫手段１０３は、設定に基づいて、電子価値情報２０１から図２（ｂ）に示すダイジェスト３０２を生成する。また、電子価値情報２０１を一方向性のハッシュ関数に通してＸ１という数を生成する。電子金庫手段１０３が持つカウンタを参照しＹ１という数を取得する。前記カウンタは参照の度に１ずつ昇順で増加し、上限に達すれば０に戻るものであるとする。これらダイジェスト３０２とハッシュ値Ｘ１とカウンタ値Ｙ１を組として登録証３０１とする。前記Ｘ１を生成するために用いたハッシュ関数として、ＭＤ５やＳＨＡ１などの分散性の高いものを用いることとする。なお、ダイジェスト３０２は空情報であってもよい。

図４は電子金庫手段１０３が電子金庫記憶手段１１０上に情報を保管する方法を示す。電子金庫手段１０３は、電子価値情報２０１をファイル８０１、登録証３０１をファイル８０２として電子金庫手段１１０に保管する。登録証３０１の構成要素であるハッシュ値Ｘ１とカウンタ値Ｙ１とファイル８０１のパス情報とファイル８０２のパス情報を組として、インデックスファイル８５２の１つのエントリとして登録する。インデックスファイル８５２は１エントリ１行のＣＳＶファイルであり、各行はカウンタ値によって昇順にソートされている。端末１００から電子金庫手段１０３に登録証が提示された場合に、電子金庫手段１０３は電子金庫記憶手段１１０中のインデックスファイル８５２から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。

ユーザが端末１００を操作して電子価値情報２０１をバックアップする手順を、

以上に示した各手段を用いて示す。以下の手順での動作は、端末１００にＩＣカード５０１を装着した状態ですべてユーザによって行なわれる。

(1-1) 端末１００が、電子情報登録手段１０６に電子価値情報リストを要求する。

(1-2) 電子情報登録手段１０６が、電子財布手段１０１に電子価値情報リストを要求する。

(1-3) 電子財布手段１０１が、電子価値情報のリストを生成し電子情報登録手段１０６に送る。

(1-4) 電子情報登録手段１０６が、前記電子価値情報リストを端末１００に送る。

(1-5) 端末１００が、前記電子価値情報リストから選択した電子価値情報２０１を電子情報登録手段１０６に要求する。

(1-6) 電子情報登録手段１０６が、電子財布手段１０１に電子価値情報２０１を要求する。

(1-7) 電子財布手段１０１が、電子価値情報２０１を電子財布記憶手段１０２から取得し、電子情報登録手段１０６に送る。

(1-8) 電子情報登録手段１０６が、電子価値情報２０１を端末１００に送る。

(1-9) 端末１００が、電子価値情報２０１の登録を電子金庫手段１０３に送る。

(1-10) 電子金庫手段１０３が、電子価値情報２０１を電子金庫記憶手段１１０に保管する。

(1-11) 電子金庫手段１０３が、登録証３０１を端末１００に送る。

(1-12) 端末１００が、登録証３０１を電子情報登録手段１０６に送る。

(1-13) 電子情報登録手段１０６が、登録証３０１の登録を電子財布手段１０１に要求する。

(1-14) 電子財布手段１０１が、電子価値情報２０１の内容と登録証３０１のダイジェスト３０２とを、電子価値情報２０１をハッシュ演算した値と登録証３０１のハッシュ値Ｘ１とを、それぞれ照合し、一致した場合に、登録証３０１を電子財布記憶手段１０２に保管し、完了通知を電子情報登録手段１０６に送る。一致しなかった場合はエラー通知を送る。

(1-15) 電子情報登録手段１０６が、電子財布手段１０１から取得した完了通知

またはエラー通知を端末１００に送る。

なお、登録証３０１が正常に電子財布記憶手段１０２に保管された場合、電子財布記憶手段１０２上から電子価値情報２０１を削除してもよい。ＩＣカードのように記憶容量が少ないデバイスを用いる場合、これは記憶容量を効率的に利用する有効な手段である。

次に、ユーザが端末１００を操作して電子財布記憶手段１０２に保管された登録証３０１に対応する電子価値情報２０１を電子財布記憶手段１０２上に復元する手順を示す。

(2-1) 端末１００が、電子情報復元手段１０７に登録証リストを要求する。

(2-2) 電子情報復元手段１０７が、電子財布手段１０１に登録証リストを要求する。

(2-3) 電子財布手段１０１が、登録証のリストを生成し電子情報復元手段１０７に送る。(2-4) 電子情報復元手段１０７が、前記登録証リストを端末１００に送る。

(2-5) 端末１００が、前記登録証リストから選択した登録証３０１を電子情報復元手段１０７に要求する。

(2-6) 電子情報復元手段１０７が、電子財布手段１０１に登録証３０１を要求する。

(2-7) 電子財布手段１０１が、登録証３０１を電子財布記憶手段１０２から取得し、電子情報復元手段１０７に送る。

(2-8) 電子情報復元手段１０７が、登録証３０１を端末１００に送る。

(2-9) 端末１００が、電子金庫手段１０３に登録証３０１を提示し、対応する電子価値情報の取得を要求する。

(2-10) 電子金庫手段１０３は登録証３０１を用いて電子価値情報２０１を検索して取得し、端末１００に送る。この時、電子金庫手段１０３は、検索した電子価値情報の内容と登録証３０１とを照合し、不整合であった場合には、電子価値情報２０１の復元処理を中止する。

(2-11) 端末１００が、電子価値情報２０１を電子情報復元手段１０７に送る。

(2-12) 電子情報復元手段１０７が、電子価値情報２０１の登録を電子財布手段１０１に要求する。

(2-13) 電子財布手段１０１が、電子価値情報２０１を電子財布記憶手段１０２条に登録する。

(2-14) 電子情報復元手段１０７が、完了通知を端末１００に送る。

以上説明したように、本実施例１の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫記憶手段上にバックアップすることと、バックアップした電子価値情報の概要を電子金庫手段に問い合わせることなく認識できることと、必要に応じて電子価値情報を電子財布記憶手段上に復元することが可能となる。

実施例２

次に、図５、図６、図７、図８、図９を用いて、本発明の請求項４、５に係る第２の実施例について説明する。図５は本実施例２における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例１（図１）で示されたシステムの端末１００を端末１１２に置き換え、電子金庫手段１０３を電子金庫手段１１３に置き換え、ＩＣカード５０１をＩＣカード５０２と置き換えたものである。ＩＣカード５０２は、ＩＣカード５０１に対して暗復号化手段１０５と鍵保管手段１０４と鍵管理手段１１５を追加し、電子情報登録手段１０６を電子情報登録手段１２０に変更し、電子情報復元手段１０７を電子情報復元手段１２１に変更したものである。

暗復号化手段１０５は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。鍵保管手段１０４は、ＥＥＰＲＯＭなどの書き換え可能なメモリによって実現される。なお、暗復号化手段１０５と電子財布手段１０１は、ＯＳとＣＰＵを共有してもよい。また、鍵保管手段１０４と電子財布記憶手段１０２は、ＥＥＰＲＯＭを共有してもよい。

鍵保管手段１０４は、図７に示すように暗号鍵４０１と復号鍵４０２を保持する。本実施例２では、鍵保管手段１０４に保管された暗号鍵４０１と復号鍵４０

２のペアは、暗復号化手段１０５が生成する。暗復号化手段１０５は、公開鍵暗号方式を用いることとし、暗号鍵４０１を公開鍵、復号鍵４０２を秘密鍵とする。なお、暗復号化手段１０５の暗号化方式として共通鍵暗号方式を用いてもよい。その場合、暗号鍵４０１と復号鍵４０２は同一の鍵となる。鍵管理手段１１５は、鍵保管手段１０４に保管された鍵を取得する機能と、鍵保管手段１０４に新しい鍵を登録する機能と、鍵保管手段１０４から既存の鍵を削除する機能を持つ。

暗復号化手段１０５は、鍵管理手段１１５を通じて鍵保管手段１０４から暗号鍵４０１を取得し、入力された電子情報を前記暗号鍵４０１で暗号化した暗号化電子情報を返す機能と、鍵管理手段１１５を通じて鍵保管手段１０４から復号鍵４０２を取得し、入力された前記暗号化電子情報を前記復号鍵４０２で復号化して前記電子情報を返す機能と、入力情報に対するハッシュ値を暗号鍵４０１を用いて暗号化した情報（電子署名）を生成する機能を持つ。また逆に、復号鍵４０２を用いて前記電子署名を検証する機能も持つ。なお、暗号鍵４０１と復号鍵４０２は、ＩＣカード５０２固有の共通鍵暗号方式の暗号鍵であってもよい。また、暗号鍵４０１と復号鍵４０２はそれぞれ、ＩＣカード５０２固有の公開鍵暗号方式の公開鍵と秘密鍵の一対の鍵ペアであってもよい。

電子情報登録手段１２０は、実施例１の電子情報登録手段１０６が持つ機能をすべて持つと同時に、図６（ａ）に示すような登録電子価値情報２０３を生成する機能を持つ。電子情報登録手段１２０は、暗復号化手段１０５を用いて電子価値情報２０１から暗号化電子価値情報２０２を取得し、電子価値情報２０１から抽出した情報を用いてダイジェスト３０２を生成し、このダイジェスト３０２と、暗号化電子価値情報２０２と、暗復号化手段１０５を用いてダイジェスト３０２と暗号化電子価値情報２０２をまとめた情報から生成した署名３０３とを、合成して登録電子価値情報２０３を生成する。また、電子情報登録手段１２０は、鍵管理手段１１５を通じて鍵保管手段１０４から鍵情報を取得する機能を持つ。

電子情報復元手段１２１は、電子情報復元手段１０７の持つ機能をすべて持つと同時に、登録電子価値情報２０３内の署名３０３を暗復号化手段１０５を用いて検証して正当性を確認した後、登録電子価値情報２０３から暗号化電子価値情

報２０２を抽出して、暗復号化手段１０５を用いて電子価値情報２０２から電子価値情報２０１を復号する機能を持つ。また、電子情報復元手段１２１は、鍵管理手段１１５を通じて鍵情報を鍵保管手段１０４に登録する機能を持つ。

電子金庫手段１１３は、図１の電子金庫手段１０３のソフトウェアを変更したものであり、電子金庫手段１１３は、電子金庫記憶手段１１０の内容の参照と変更を行なうことができる。電子金庫手段１１３が登録電子価値情報２０３の登録要求を受けた場合、図６（ｂ）に示す登録証３０４を登録電子価値情報２０３を用いて生成する。登録証３０４を生成する処理の流れを以下に説明する。

電子金庫手段１１３は、登録電子価値情報２０３からダイジェスト３０２を抽出する。また、暗号化電子価値情報２０２を一方向性のハッシュ関数に通してＸ２という数を生成する。電子金庫手段１１３が持つカウンタを参照しＹ２という数を取得する。前記カウンタは参照の度に１ずつ昇順で増加し、上限に達すれば０に戻るものであるとする。これらダイジェスト３０２とハッシュ値Ｘ２とカウンタ値Ｙ２を組として登録証３０４とする。前記Ｘ２を生成するために用いたハッシュ関数として、ＭＤ５やＳＨＡ１などの分散性の高いものを用いることとする。登録証３０４はダイジェスト３０２の情報を含むため、それを参照することで登録された電子価値情報の概要を把握することができる。なお、ダイジェスト３０２は空情報の場合もあってもよいが、その場合は登録証３０４から電子価値情報の概要を知ることはできない。

また、電子金庫手段１１３が復号鍵４０２の登録要求を受けた場合、図８（ａ）に示す登録証３０５を生成する。登録証３０５は、鍵情報に対する登録証であることを示すダイジェスト３０６と、復号鍵４０２から生成したハッシュ値Ｘ３と、電子金庫手段１１３が持つカウンタ値Ｙ３とから構成される。ダイジェスト３０６は、図８（ｂ）に示すように、鍵情報に対する登録証であることを示す情報種別と鍵情報とからなる。

電子価値情報に対する登録証３０４と、鍵情報に対する登録証３０５との区別は、電子価値情報に対する登録証３０４に含まれる情報種別と鍵情報に対応する登録証３０５に含まれる情報種別の違いによって行う。これにより、電子金庫手

段１１３が電子価値情報と鍵情報を電子金庫記憶手段１１０に格納する際に、両者に対して同じ管理方法を用いることができる。図９はその管理方法を示した図である。

電子金庫手段１１３は、実施例１における電子金庫手段１０３の機能をすべて持つと同時に、登録電子価値情報２０３をファイル８０３、登録証３０４をファイル８０４、復号鍵４０２をファイル８０５、登録証３０５をファイル８０６として、それぞれ電子金庫記憶手段１１０に保管する。登録証３０４の構成要素であるハッシュ値Ｘ２とカウンタ値Ｙ２とファイル８０３のパス情報とファイル８０４のパス情報を組として、インデックスファイル８５３の１つのエントリとして登録する。また、登録証３０５の構成要素であるハッシュ値Ｘ３とカウンタ値Ｙ３とファイル８０５のパス情報とファイル８０６のパス情報を組として、インデックスファイル８５３の１つのエントリとして登録する。インデックスファイル８５３は１エントリ１行のＣＳＶファイルであり、各行はカウンタ値によって昇順にソートされている。端末１１２から電子金庫手段１１３に登録証が提示された場合に、電子金庫手段１１３は、電子金庫記憶手段１１０中のインデックスファイル８５３から登録証に対応する電子価値情報をカウンタ値の一致するエントリ群を検索し、その中からハッシュ値が一致するエントリ群にさらに絞り込み、登録証が完全に一致するエントリを抽出する。これにより登録証に対応する電子価値情報を高速に検索することが可能である。なお、電子価値情報と鍵情報のインデックスファイルを分けても良い。

次に、ユーザが端末１１２を操作して電子価値情報２０１をバックアップする手順を示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(1-1) 端末１１２が、電子情報登録手段１２０に電子価値情報リストを要求する。

(1-2) 電子情報登録手段１２０が、電子財布手段１０１に電子価値情報リストを要求する。

(1-3) 電子財布手段１０１が、電子価値情報のリストを生成し電子情報登録手段１２０に送る。

(1-4) 電子情報登録手段１２０が、前記電子価値情報リストを端末１１２に送る。

(1-5) 端末１１２が、前記電子価値情報リストから選択した電子価値情報２０１の選択を電子情報登録手段１２０に通知する。

(1-6) 電子情報登録手段１２０が、電子財布手段１０１に電子価値情報２０１を要求する。

(1-7) 電子財布手段１０１が、電子価値情報２０１を電子財布記憶手段１０２から取得し、電子情報登録手段１２０に送る。

(1-8) 電子情報登録手段１２０が、暗復号化手段１０５を用いて電子価値情報２０１から暗号化電子価値情報２０２を取得し、電子価値情報２０１と暗号化電子価値情報２０２から登録電子価値情報２０３を生成する。

(1-9) 電子情報登録手段１２０が、登録電子価値情報２０３を端末１１２に送る。

(1-10) 端末１１２が、登録電子価値情報２０３の登録を電子金庫手段１１３に要求する。

(1-11) 電子金庫手段１１３が、登録電子価値情報２０３を電子金庫記憶手段１１０に保管すると同時に、登録電子価値情報２０３から登録証３０４を生成する。

(1-12) 電子金庫手段１１３が、登録証３０４を端末１００に送る。

(1-13) 端末１１２が、登録証３０４を電子情報登録手段１２０に送る。

(1-14) 電子情報登録手段１２０が、登録証３０４の登録を電子財布手段１０１に要求する。

(1-15) 電子財布手段１０１が、電子価値情報２０１の内容から生成したダイジェストと登録証３０４のダイジェスト３０２とを、前記ダイジェストをハッシュ演算した値と登録証３０４のハッシュ値Ｘ２とを、それぞれ照合し、一致した場合に、登録証３０４を電子財布記憶手段１０２に保管し、完了通知を電子情報登録手段１２０に送る。一致しなかった場合はエラー通知を送る。

(1-16) 電子情報登録手段１２０が、電子財布手段１０１から取得した完了通知またはエラー通知を端末１１２に送る。

次に、ユーザが端末１１２を操作して電子財布記憶手段１０２に保管された登録証３０４に対応する電子価値情報２０１を電子財布記憶手段１０２上に復元する手順を示す。

(2-1) 端末１１２が、電子情報復元手段１２１に登録証リストを要求する。

(2-2) 電子情報復元手段１２１が、電子財布手段１０１に登録証リストを要求する。

(2-3) 電子財布手段１０１が、登録証のリストを生成し電子情報復元手段１２１に送る。(2-4) 電子情報復元手段１２１が、前記登録証リストを端末１１２に送る。

(2-5) 端末１１２が、前記登録証リストから選択した登録証３０４を電子情報復元手段１２１に要求する。

(2-6) 電子情報復元手段１２１が、電子財布手段１０１に登録証３０４を要求する。

(2-7) 電子財布手段１０１が、登録証３０４を電子財布記憶手段１０２から取得し、電子情報復元手段１２１に送る。

(2-8) 電子情報復元手段１２１が、登録証３０４を端末１１２に送る。

(2-9) 端末１１２が、電子金庫手段１１３に登録証３０４を提示し、対応する電子価値情報の取得を要求する。

(2-10) 電子金庫手段１０３は登録証３０４を用いて登録電子価値情報２０３を検索して取得し、端末１１２に送る。この時、電子金庫手段１０３は、検索した電子価値情報の内容と登録証３０４とを照合し、不整合であった場合には、電子価値情報２０１の復元処理を中止する。

(2-11) 端末１１２が、登録電子価値情報２０３を電子情報復元手段１２１に送る。

(2-12) 電子情報復元手段１２１が、暗復号化手段１０５を用いて登録電子価値情報２０３の署名３０３を検証し、成功したとき、登録電子価値情報２０３から抽出した暗号化電子価値情報２０２を暗復号化手段１０５を用いて復号化して電子価値情報２０１を取得する。

(2-13) 電子情報復元手段１２１が、電子価値情報２０１の登録を電子財布手段１０１に要求する。

(2-14) 電子財布手段１０１が電子価値情報２０１を電子財布記憶手段１０２に

登録する。

(2-15) 電子情報復元手段１２１が、完了通知を端末１１２に送る。

また、ユーザが端末１１２を操作して復号鍵４０２をバックアップする手順を次に示す。以下の手順での選択動作はすべてユーザによって行なわれる。

(3-1) 端末１１２が、復号鍵４０２を電子情報登録手段１２０に要求する。

(3-2) 電子情報登録手段１２０が、鍵管理手段１１５に復号鍵４０２を要求する。

(3-3) 鍵管理手段１１５が、復号鍵４０２を鍵保管手段１０４から取得し、電子情報登録手段１２０に送る。

(3-4) 電子情報登録手段１２０が、復号鍵４０２を端末１１２に送る。

(3-5) 端末１１２が、復号鍵４０２を電子金庫手段１１３に登録を要求する。

(3-6) 電子金庫手段１１３が、復号鍵４０２を電子金庫記憶手段１１０に保管すると同時に、登録証３０５を生成する。

(3-7) 電子金庫手段１１３が、登録証３０５を端末１１２に送る。

(3-8) 端末１１２が、登録証３０５を電子情報登録手段１２０に送る。

(3-9) 電子情報登録手段１２０が、登録証３０５の登録を電子財布手段１０１に要求する。

(3-10) 電子財布手段１０１が、登録証３０５を電子財布記憶手段１０２に保管し、完了通知を電子情報登録手段１２０に送る。

(3-11) 電子情報登録手段１２０が、電子財布手段１０１から取得した完了通知またはエラー通知を端末１１２に送る。

次に、ユーザが端末１１２を操作して電子財布記憶手段１０２に保管された登録証３０５に対応する復号鍵４０２を鍵保管手段１０４上に復元する手順を示す。

(4-1) 端末１１２が、電子情報復元手段１２１に登録証リストを要求する。

(4-2) 電子情報復元手段１２１が、電子財布手段１０１に登録証リストを要求する。

(4-3) 電子財布手段１０１が、登録証のリストを生成して電子情報復元手段１２１に送る。

(4-4) 電子情報復元手段１２１が、前記登録証リストを端末１１２に送る。

(4-5) 端末１１２が、前記登録証リストから選択した登録証３０５を電子情報復元手段１２１に要求する。

(4-6) 電子情報復元手段１２１が、電子財布手段１０１に登録証３０５を要求する。

(4-7) 電子財布手段１０１が、登録証３０５を電子財布記憶手段１０２から取得し、電子情報復元手段１２１に送る。

(4-8) 電子情報復元手段１２１が、登録証３０５を端末１１２に送る。

(4-9) 端末１１２が、電子金庫手段１１３に登録証３０５を提示し、対応する復号鍵の取得を要求する。

(4-10) 電子金庫手段１０３は登録証３０５を用いて復号鍵４０２を検索して取得し、端末１１２に送る。

(4-11) 端末１１２が、復号鍵４０２を電子情報復元手段１２１に送る。

(4-12) 電子情報復元手段１２１が、復号鍵４０２の登録を鍵管理手段１１５に要求する。

(4-13) 鍵管理手段１１５が復号鍵４０２を鍵保管手段１０４に登録する。

(4-14) 電子情報復元手段１２１が、完了通知を端末１１２に送る。

なお、電子情報登録手段１２０と電子金庫手段１１３の通信は、端末１１２を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１２も通信されている情報の内容を知ることはできない。また、電子情報復元手段１２１と電子金庫手段１１３の通信は、端末１１２を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１２も通信されている情報の内容を知ることはできない。

以上説明したように、本実施例２の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を電子金庫手段に保管することで、鍵保管手段が壊れた場合にも電子価値情報を復元することが可能になる。

実施例３

次に、図１０を用いて本発明の請求項６に係る第３の実施例について説明する。図１０は本実施例３における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例２（図５）で示されたシステムの端末１１２を端末１１４に置き換え、端末１１４と通信する電子金庫手段１２３と、電子金庫手段１２３の記憶装置である電子金庫記憶手段１２２を追加したものである。電子金庫手段１２３と電子金庫記憶手段１２２は、電子金庫手段１１３と電子金庫記憶手段１１０と同等の機能を持つ。端末１１４は、端末１１２が持つ機能をすべて持つと同時に、電子金庫手段１２３に対しても電子価値情報および復号鍵のバックアップ先とする機能を持つ。

本実施例３では、電子金庫手段１１３に対して電子価値情報２０１から生成される登録電子価値情報２０３のバックアップを行い、電子金庫手段１２３に対して復号鍵４０２のバックアップを行うこととする。復号鍵４０２のバックアップ手順は、バックアップ先を電子金庫手段１１３から電子金庫手段１２３に変更したことを除いて、実施例２と同じ方式を用いることとする。このため、電子金庫手段１１３と電子金庫手段１２３が共謀することがない限り、電子金庫手段１１３と電子金庫手段１２３には電子価値情報２０１を解読されない。

なお、電子情報登録手段１２０と電子金庫手段１１３の通信は、端末１１４を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１４も通信されている情報の内容を知ることはできない。また、電子情報復元手段１２１と電子金庫手段１１３の通信は、端末１１４を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１４も通信されている情報の内容を知ることはできない。

さらに、電子情報登録手段１２０と電子金庫手段１２３の通信は、端末１１４を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１４も通信されている情報の内容を知ることはできない。また、電子情報復元手段１２１と電子金庫手段１２３の通信は、端末１１４を含めた通信路での盗聴を防ぐために、暗号化通信を行ってもよい。この場合、端末１１４も通信さ

れている情報の内容を知ることはできない。

以上説明したように、本実施例３の電子情報バックアップシステムによれば、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を暗号化した電子価値情報と別の電子金庫手段に保管することで、二つの電子金庫手段が共謀しない限り元の電子価値情報を取得できないようにすることが可能となる。

実施例４

次に、図１１を用いて、本発明の請求項７、８、９に係る第４の実施例について説明する。図１１は本実施例４における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例３（図１０）で示されたシステムの端末１１４を端末１１６に置き換え、ＩＣカード５０２をＩＣカード５０３と置き換えたものである。ＩＣカード５０３は、ＩＣカード５０２に対して電子情報分割手段１２６と電子情報合成手段１２７を追加し、電子情報登録手段１２０を電子情報登録手段１２４に変更し、電子情報復元手段１２１を電子情報復元手段１２５に変更したものである。電子情報分割手段１２６および電子情報合成手段１２７は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。

以下、本実施例４の動作について説明するが、基本的な動作は上記実施例２および３と同様であるので、以下には実施例２および３と異なる部分についてのみ説明する。電子情報分割手段１２６は、電子価値情報を元の電子価値情報へ復元するための識別子を付加した任意の数の部分電子情報に分割する。電子情報合成手段１２７は、この分割電子情報のすべてから元の電子価値情報を復元する。電子情報登録手段１２４は、電子価値情報の分割を電子情報分割手段１２６に要求して複数の部分電子情報を取得するとともに、その部分電子情報のすべてを電子金庫手段１１３に登録して同数の部分情報登録証を取得する。そして、電子情報復元手段１２５は、取得した部分情報登録証のすべてをそれぞれの部分情報登録

証に対応する電子金庫手段１１３に提示して同数の部分電子情報を取得し、電子情報合成手段１２７が、その取得した部分電子情報のすべてから電子価値情報を電子財布手段１０１上に復元する。

本実施例４では、電子情報登録手段１２４は、登録する分割電子情報を暗復号化手段１０５を用いて暗号化して暗号化分割電子情報を取得し、取得した暗号化分割電子情報を電子金庫手段１１３に登録して対応する登録証を取得するようにしているが、逆に、電子価値情報を暗復号化手段１０５を用いて暗号化して暗号化電子情報を取得し、取得した暗号化電子情報を電子情報分割手段１２６を用いて分割暗号化電子情報を取得するとともに、その分割暗号化電子情報を電子金庫１１３に登録して対応する登録証を取得するようにしてもよい。また、上記実施例３のように、電子金庫手段１１３に対しては暗号化分割電子情報のバックアップを行い、電子金庫手段１２３に対しては復号鍵のバックアップを行うようにしてもよい。

実施例５

次に、図１２を用いて、本発明の請求項１０に係る第５の実施例について説明する。図１２は本実施例５における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例３（図１０）で示されたシステムの端末１１４を端末１１７に置き換え、ＩＣカード５０２をＩＣカード５０４に置き換えたものである。ＩＣカード５０４は、ＩＣカード５０２に対して電子情報結合手段１３０と電子情報結合解除手段１３１を追加し、電子情報登録手段１２０を電子情報登録手段１２８に変更し、電子情報復元手段１２１を電子情報復元手段１２９に変更したものである。電子情報結合手段１３０は、複数の電子価値情報を結合して一つの結合電子情報として出力する。電子情報結合解除手段１３１は、結合電子情報を複数の元の電子情報に分離する。電子情報結合手段１３０および電子情報結合解除手段１３１は、ソフトウェアと、このソフトウェアを格納する記憶領域と、このソフトウェアを解釈して実行するためのＯＳおよびＣＰＵによって構成される。

以下、本実施例５の動作について説明するが、基本的な動作は上記実施例３と

同様であるので、以下には実施例３と異なる部分についてのみ説明する。電子情報結合手段１３０は、複数の電子価値情報の組から１つの結合電子情報を生成し、電子情報登録手段１２８が、この結合電子情報を電子金庫手段１１３に登録して対応する結合電子情報登録証を取得し、電子情報復元手段１２９が、この結合電子情報登録証を提示して電子金庫手段１１３から対応する結合電子情報を取得し、電子情報結合解除手段１３１が、この結合電子情報から元の複数の電子価値情報の組を生成して電子財布手段１０１上に復元する。

本実施例５では、電子情報登録手段１２８は、登録する結合電子情報を暗復号化手段１０５を用いて暗号化して結合暗号化電子情報を取得し、取得した結合暗号化電子情報を電子金庫手段１１３に登録して対応する登録証を取得するようにしているが、逆に、複数の電子価値情報をそれぞれ暗復号化手段１０５を用いて暗号化して暗号化電子情報を取得し、取得した暗号化電子情報を電子情報結合手段１３０を用いて結合暗号化電子情報を電子金庫手段１１３に登録して対応する登録証を取得するようにしてもよい。また、上記実施例３のように、電子金庫手段１１３に対しては結合暗号化電子情報のバックアップを行い、電子金庫手段１２３に対しては復号鍵のバックアップを行うようにしてもよい。

実施例６

次に、図１３を用いて、本発明の請求項１１、１２に係る第６の実施例について説明する。図１３は本実施例６における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例４（図１１）と実施例５（図１２）で示されたシステムを結合したものであり、新たな端末１１８とＩＣカード５０５を用いたものである。ＩＣカード５０５は、電子情報登録手段１３２および電子情報復元手段１３３と、電子分割手段１３４および電子合成手段１３５と、電子情報結合手段１３６および電子情報結合解除手段１３７とを備えている。その他は実施例４および５と同じである。

以下、本実施例６の動作について説明するが、本実施例６が上記実施例４、５と異なるのは、本実施例６では、復号鍵を２つの部分鍵に分割するとともに、一方の部分鍵を電子価値情報と組にして一方の電子金庫手段１１３に登録し、他方

の部分鍵を他方の電子金庫手段１２３に登録することである。電子情報分割手段１３４は、電子情報登録手段１３２が鍵保管手段１０４から鍵管理手段１０５を通じて取得した復号鍵情報を複数の部分鍵に分割する。暗復号化手段１０５は、電子情報登録手段１３２が電子財布手段１０１から取得した電子価値情報を暗号化して暗号化電子情報を取得する。電子情報結合手段１３６は、これら暗号化電子情報と分割された部分鍵の一部である部分鍵群Ａとを結合して結合電子情報を出力する。電子情報登録手段１３２は、この結合電子情報を電子金庫手段１１３に、残りの部分鍵である部分鍵群Ｂを別の電子金庫手段１２３に登録してそれぞれ対応する登録証を取得する。電子情報復元手段１３３は、それらの登録証を対応する電子金庫手段１１３および１２３に提示して結合電子情報と部分鍵群Ｂとを取得する。電子情報結合解除手段１３７は、その結合電子情報を暗号化電子情報と部分鍵群Ａとに分離し、電子情報合成手段１３５は、部分鍵群Ａと部分鍵群Ｂとを合成して復号鍵を生成し、暗複合化手段１０５は、暗号化電子情報を復号して電子価値情報を出力し、電子情報復元手段１３３は、その鍵情報を鍵管理手段１１５を通じて鍵保管手段１０４上に復元するとともに、電子価値情報を電子財布手段１０１上に復元する。

上記した説明は、電子価値情報を２つに分割した例であるが、３つ以上のさらに多くに分割してもよい。また、分割した電子価値情報を１つの電子金庫手段にのみ預けるようにしてもよい。また、分割した電子価値情報の全てを預ける必要は必ずしもなく、必要なものだけを預けるようにしてもよい。さらに、上記実施例４のように、電子価値情報自体を複数に分割して、一方の分割電子情報を一方の分割鍵情報と組み合わせて一方の電子金庫手段１１３に登録し、他方の分割電子情報を他方の分割鍵情報と組み合わせて他方の電子金庫手段１２３に登録するようにしてもよい。また、上記実施例５のように、電子価値情報として複数の電子価値情報を組み合わせた電子価値情報を使用するようにしてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化して

バックアップした電子価値情報を電子金庫手段から復元することと、復号鍵を分割して、一方の分割鍵を電子価値情報とともに一方の電子金庫サーバにバックアップし、他方の分割鍵を他方の電子金庫サーバにバックアップすることで、復号鍵の一部を取得しただけでは、暗号化された電子価値情報を解読することはできないので、安全に鍵情報ひいては電子価値情報をバックアップすることが可能となる。

実施例７

次に、図１４を用いて、本発明の請求項１３に係る第７の実施例について説明する。図１４は本実施例７における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例６（図１３）で示されたＩＣカード５０５をＩＣカード５０６に置き換えたものである。ＩＣカード５０６は、ＩＣカード５０５に対して、鍵管理手段１３８の管理の基に、鍵保管手段１３９が、復号鍵を数学的に生成するために用いる元の暗号種（たね）情報１４０と、この暗号種情報から復号鍵を生成する復号鍵生成アルゴリズム１４１とを保持している。暗復号化手段１４２は、暗号種情報１４０に復号鍵生成アルゴリズム１４１をかけて復号鍵を生成する。暗号種情報１４０および復号鍵生成アルゴリズム１４１は、始めから鍵保管手段１３９に保持してもよく、またはどちらか一方を保持して、後から他方を外部からダウンロードしてもよく、両方とも外部からダウンロードしてもよい。暗号種情報としては、素数やその他の公知のものが使用可能であり、復号鍵だけでなく、暗号鍵と復号鍵の鍵ペアを数学的に生成する元となる情報としてもよい。

以下、本実施例７の動作について説明するが、基本的な動作は上記実施例１から６と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。

(1-1) 端末１１８が、暗復号化手段１４２に対して復号鍵の取得を要求する。

(1-2) 暗復号化手段１４２は、鍵管理手段１３８を通じて鍵保管手段１３９を参照し、暗号種情報１４０を取得する。

(1-3) 暗復号化手段１４２は、暗号種情報１４０を電子情報登録手段１３２に渡

す。

(1-4) 電子情報登録手段１３２は、端末１１８を通じて電子金庫手段１２３に暗号種情報１４０の登録を要求する。

(1-5) 電子金庫手段１２３は、暗号種情報１４０を電子金庫記憶手段１２２に格納し、端末１１８に暗号種情報登録証を送付して登録完了を通知する。

(1-6) 端末１１８は、暗号種登録証を電子情報登録手段１３２に渡す。

(1-7) 鍵管理手段１３８は、暗号種登録証を鍵保管手段１３９に渡し、鍵保管手段１３９から暗号種情報１４０を削除する。

(2-1) 端末１１８が、電子財布手段１０１に電子価値情報リストを要求する。電子財布手段１０１は、電子価値情報のリストを生成し、端末１１８に送る。

(2-2) 端末１１８は、電子価値情報リストから選択した電子価値情報の提供を電子財布手段１０１に要求する。電子財布手段１０１は、電子価値情報を電子財布記憶手段１０２から取得する。暗号化手段１４２は、電子価値情報から暗号化電子価値情報を生成し、電子財布手段１０１に送る。電子財布手段１０１は、暗号化電子価値情報を電子登録手段１３２を通じて端末１１８に送る。

(2-3) 端末１１８は、暗号化電子価値情報の登録を電子金庫手段１１３に要求する。電子金庫手段１１３は、暗号化電子価値情報を電子金庫記憶手段１１０に保管するとともに、電子情報登録証を生成し、その登録証を端末１１８に送る。

(2-4) 端末１１８は、電子情報登録証の保管を電子情報登録手段１３２を通じて電子財布手段１０１に要求する。電子財布手段１０１は、電子情報登録証を電子財布記憶手段１０２に保管し、完了通知を端末１１８に送る。

(3-1) 端末１１８が、電子情報復元手段１３３を通じて暗復号化手段１４２に復号鍵を要求する。

(3-2) 鍵管理手段１３８は、鍵保管手段１３９から暗号種情報登録証を抽出して、暗復号化手段１４２に渡す。

(3-3) 暗復号化手段１４２は、暗号種情報登録証を電子情報復元手段１３３に渡し、端末１１８は、電子情報復元手段１３３を通じて、電子金庫手段１２３に暗号種情報登録証を提示して暗号種情報の返還を要求する。

(3-4) 電子金庫手段１２３は、暗号種情報登録証から該当する暗号種情報を電子金庫記憶手段１２２から取り出し、端末１１８に渡す。

(3-5) 暗復号化手段１４２は、鍵管理手段１３８を通じて鍵保管手段１３９から復号鍵生成アルゴリズム１４１を受け取るとともに、その復号鍵生成アルゴリズム１４１を、電子情報復元手段１３３を通じて受け取った暗号種情報にかけて復号鍵を生成する。

(3-6) 暗復号化手段１４２は、復元した復号鍵を鍵管理手段１３８を通じて鍵保管手段１３９に保管する。

(3-7) 暗復号化手段１４２は、復号鍵の復元が完了したことを端末１１８に通知する。

なお、本実施例７では、電子価値情報を電子金庫手段１１３に登録し、暗号種情報を電子金庫手段１２３に登録したが、両者を１つの電子金庫手段に登録してそれぞれについての登録証を受領するようにしてもよい。また、上記実施例６のように、暗号種情報を電子分割手段１３４により分割して、その一方を電子結合手段１３６により電子価値情報と組み合わせて電子金庫手段１１３に登録し、他方の分割種情報を他方の電子金庫手段１２３に登録し、復元時には、電子金庫手段１１３から受け取った電子価値情報を電子結合解除手段１３７により電子価値情報と一方の種情報とに分離し、この分離した種情報と、電子金庫手段１２３から受け取った他方の種情報を電子情報結合手段１３５により結合して１つの種情報としてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、暗号化を解読する復号鍵そのものをバックアップするのでなく、その元となる暗号種情報をバックアップすることで、暗号種情報を取得しただけでは復号することができないので、極めて安全に鍵情報ひいては電子価値情報をバックアップすることが可能となる。

実施例８

次に、図１５を用いて、本発明の請求項１４に係る第８の実施例について説明する。図１５は本実施例７における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例６（図１３）で示されたシステムの端末１１８を端末１１９に置き換え、ＩＣカード５０５をＩＣカード５０７と置き換えたものである。ＩＣカード５０７は、ＩＣカード５０５に対して電子情報登録手段１３２を電子情報登録手段１４３に変更し、電子情報復元手段１３３を電子情報復元手段１４４に変更したものである。端末１１９には、所有者情報入力手段１４５と所有者認証情報入力手段１４６が接続されている。

以下、本実施例８の動作について説明するが、基本的な動作は上記実施例１から６と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末１１９には、所有者情報入力手段１４５から所有者固有の所有者情報を入力するとともに、所有者認証情報入力手段１４６から所有者情報に対応する所有者認証情報を入力する。電子情報登録手段１４３は、電子価値情報と所有者認証情報入力手段１４６より取得した所有者認証情報とを組として電子金庫手段１１３に登録する。電子情報復元手段１４４は、所有者情報入力手段１４５より取得した所有者情報を電子金庫手段１１３に提示し、所有者認証情報との照合が成功した時に、電子価値情報を取得することができる。なお、所有者情報と所有者認証情報とは、同一の情報を用いて単純に比較することでもよく、所有者認証情報として所有者情報を一方向性関数で計算した値を用いてもよい。また、所有者情報としてパスワードを用いてもよく、また、指紋や掌紋、虹彩などの生体情報を用いてもよい。

以上に説明したシステムを用いることで、ユーザが持つ電子価値情報を電子金庫手段には秘密の鍵を用いて暗号化してバックアップすることと、バックアップした電子価値情報の概要をローカルで把握することと、必要に応じて暗号化してバックアップした電子価値情報を電子金庫手段から復元することと、前記の暗号化を解読する復号鍵を紛失した場合にも、認証が成功すればその鍵を鍵保管手段上に復元することで暗号化された電子価値情報を復号することと、安全な方法で

認証を実現することが可能となる。

実施例９

次に、図１６を用いて、本発明の請求項１５、１６、１７に係る第９の実施例について説明する。図１６は本実施例９における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例８（図１５）で示されたシステムの端末１１９を端末１４７に置き換え、この端末１４７に、所有者情報入力手段１４５と所有者認証情報保管手段１４８と所有者認証手段１４９とを接続したものである。

以下、本実施例９の動作について説明するが、基本的な動作は上記実施例１から６と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末１４７には、所有者情報入力手段１４５から所有者固有の所有者情報が入力される。所有者認証情報保管手段１４８は、入力された所有者情報に対応する所有者認証情報が保持されている。所有者認証手段１４９は、入力された所有者情報と保管された所有者認証情報とを対照して正当性を検証する。検証の結果、正当な所有者と認証された場合は、端末１４７は、そのことを電子金庫手段１１３に通知し、電子金庫手段１１３は、電子情報登録手段１４３と電子金庫手段１１３との間の暗号化通信路を構築する。電子情報登録手段１４３は、この暗号化通信路を通して電子価値情報を電子金庫手段１１３に登録し、電子金庫手段１１３は、認証結果に対応する所有者認証情報と電子価値情報とを組として電子金庫記憶手段１１０に保持する。これにより、電子情報復元手段１４４は、上記の暗号化通信路を通して認証結果に基づく所有者認証情報に対応した電子価値情報を取得することができる。

なお、所有者情報入力手段１４５と所有者認証手段１４９が一時的に利用する共通鍵を生成して共有し、この共通鍵によって所有者情報を暗号化して所有者認証手段１４９に送信するようにしてもよい。また、所有者情報入力手段１４５が、所有者認証手段１４９固有の秘密鍵に対応した公開鍵で所有者情報を暗号化し、この暗号化した所有者情報を所有者認証手段１４９に送信するようにしてもよい。

また、所有者情報と所有者認証情報とは、同一の情報を用いて単純に比較する

ようにしてもよく、所有者認証情報として所有者情報を一方向性関数で計算した値を用いてもよい。また、所有者情報としてパスワードを用いてもよく、指紋や掌紋、虹彩などの生体情報を用いてもよい。

実施例１０

次に、図１７を用いて、本発明の請求項１８、１９に係る第１０の実施例について説明する。図１７は本実施例１０における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例８（図１５）で示されたシステムの端末１１９を端末１５０に置き換え、この端末１５０に認証機器読み取り手段１５１を接続するとともに、電子金庫手段１１３を電子金庫手段１５２に置き換えたものである。認証機器読み取り手段１５１は、認証機器としてのＩＣカードを読み取るためのＩＣカードリーダである。また、電子金庫手段１５２には、認証確認情報保管手段１５３からの情報を基に、認証機器としてのＩＣカードの正当性を検証するための認証確認手段１５４が接続されている。

以下、本実施例１０の動作について説明するが、基本的な動作は上記実施例１から６と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。端末１５０には、認証機器読み取り手段１５１が読み取った認証機器としてのＩＣカードのＩＤ情報が入力される。端末１５０は、このＩＤ情報を電子金庫手段１５２に送る。電子金庫手段１５２は、そのＩＤ情報を認証確認手段１５４に送ると、認証確認手段１５４は、認証確認情報保管手段１５３から対応するＩＤ情報を読み出して対照して正当性を検証する。検証の結果、正当な所有者と認証された場合は、電子金庫手段１５２は、その情報を端末１５０に送り、電子情報登録手段１４３と電子金庫手段１５２との間の暗号化通信路を構築するとともに、この暗号化通信路を通して電子情報登録手段１４３が電子価値情報を電子金庫手段１５２に登録する。電子金庫手段１５２は、認証結果に対応する所有者認証情報と電子価値情報とを組として電子金庫記憶手段１１０に保持する。これにより、電子情報復元手段１４４は、上記の暗号化通信路を通して認証結果に基づく所有者認証情報に対応した電子価値情報を取得することができる。

なお、本実施例１０では、認証機器としてＩＣカードを用い、認証機器読み取

り手段としてＩＣカードリーダを用いているが、セキュリティ機能を有するメモリカードとメモリカードリーダを用いてもよい。

実施例１１

次に、図１８を用いて、本発明の請求項２０、２１に係る第１１の実施例について説明する。図１８は本実施例１１における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例８（図１５）で示されたシステムの端末１１９を端末１６０に置き換え、ＩＣカード５０７をＩＣカード５０８に置き換え、電子情報登録手段１４３を電子登録手段１５５に置き換え、電子情報復元手段１４４を電子情報復元手段１５６に置き換え、電子財布手段１０１を電子財布手段１５７に置き換え、さらに、電子価値情報をバックアップする条件情報を保持するバックアップ条件保管手段１５８およびバックアップ条件保管手段１５８から取得したバックアップ条件を解釈して電子財布手段１５７からバックアップ対象を選択するバックアップ対象抽出手段１５９とを追加し、端末１１９を端末１５０に置き換えたものである。電子情報登録手段１４５は、バックアップ対象の電子価値情報を自動的に電子金庫手段１１３に登録して対応する登録証を取得する。これによってバックアップする電子価値情報の選択を、ユーザによる手動選択ではなく事前に設定した条件に基づいて自動的に行なうことができる。

以下、本実施例１１の動作について説明するが、基本的な動作は上記実施例１から６と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。バックアップ条件保管手段１５８は、バックアップ条件情報を保持し、その条件情報に基づいて、バックアップする電子価値情報を決定する。本実施例１１では、バックアップ条件情報には初期設定が存在し、また条件情報をユーザが作成・変更できるものとする。バックアップ条件情報としては、電子価値情報の種類や容量、電子財布記憶手段１０２の空きメモリ容量、電子価値情報の有効期限、電子価値情報の保持開始時間等およびそれらの組み合わせを用いることができる。なお、電子価値情報が持つ情報の項目にあわせて、前記した以外の情報をバックアップ条件に用いても良い。

バックアップ条件情報の例を図１９と図２０で示す。図１９は電子財布記憶手段１０２上の電子価値情報群の例である。ここでバックアップ条件を映画のチケットとした場合、図２０（ａ）は上記バックアップ条件に対応する電子価値情報群を示す。本日の日付を２０００年３月１５日として、一ヶ月以内に使用可能な日がないことをバックアップ条件とした場合の対応する電子価値情報群は図２０（ｂ）で示される。

次に、このようなバックアップ条件に基づくバックアップ対象抽出手段１５９による電子価値情報の抽出手順について説明する。

(2-1) バックアップ対象抽出手段１５９が電子財布手段１５７に電子価値情報のリストを要求する。

(2-2) 電子財布手段１５７が電子財布記憶手段１０２を参照し、電子価値情報のリストを構成する。

(2-3) 電子財布手段１５７が電子価値情報のリストをバックアップ対象抽出手段１５９に返す。

(2-4) バックアップ対象抽出手段１５９は登録されたバックアップ条件とリストを照合し、バックアップ対象電子価値情報リストを生成する。

(2-5) バックアップ対象抽出手段１５９は電子財布手段１５７にバックアップ対象電子価値情報リストを渡す。

(2-6) 電子財布手段１５７は電子財布記憶手段１０２からバックアップ対象電子価値情報リストで指定された電子価値情報群を取得する。

(2-7) 電子価値情報群に含まれるすべての電子価値情報をそれぞれ暗復号化手段１０５を用いて暗号化し、暗号化電子価値情報群を生成する。

(2-8) 暗号化電子価値情報群に含まれるすべての暗号化電子価値情報を電子情報登録手段１５５から端末１６０を経由して、電子金庫手段１１３にバックアップする。

(2-9) 電子金庫手段１１３から暗号化電子価値情報群に対応する登録証群を端末１６０から電子情報復元手段１５６を経由して電子財布手段１５７に渡す。

(2-10) 電子財布手段１５７は登録証群を電子財布記憶手段１０２に保管し、電

子財布記憶手段１０２上から電子価値情報群に含まれる電子価値情報をすべて削除する。

(2-11)　電子財布記憶手段１５７は端末１６０に完了を通知する。

バックアップ対象抽出手段１５９を起動させるタイミングとしては、例えば一定時間ごとにバックアップ対象抽出手段１４９を起動して、自動的に上記(2-1)から(2-11)で示した手順に従ってバックアップを開始してもよい。または、新規の電子価値情報が電子財布記憶手段に登録される時やバックアップされていた電子価値情報を復元する時に、電子財布記憶手段１０２の記憶容量が不足する場合にバックアップ対象抽出手段１５９が自動的に前記手順にしたがってバックアップを開始してもよい。または、ユーザによる起動要求があった場合に、バックアップ対象抽出手段１５９が自動的に上記手順にしたがってバックアップを開始してもよい。または、上記の条件の組み合わせによって、バックアップ対象抽出手段１５９が自動的に上記手順にしたがってバックアップを開始してもよい。

また、電子財布記憶手段１０２の記憶容量不足の場合、現在の電子財布記憶手段１０２に保持された電子価値情報をバックアップ条件情報に基づいてバックアップする処理を行なった上で、新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することと、新規の電子価値情報の登録やバックアップ済み電子価値情報の復元を中断することと、手動で現在の電子財布記憶手段１０２に保持された電子価値情報を選択しバックアップする処理を行なった上で、新規の電子価値情報の登録やバックアップ済みの電子価値情報の復元を継続することを、端末１６０を操作するユーザに選択させても良い。

実施例１２

次に、図２１を用いて、本発明の請求項２２、２３に係る第１２の実施例について説明する。図２１は本実施例１２における電子情報バックアップシステムの一例を示した構成図であり、本システムは実施例３（図１０）で示されたシステムの端末１１４を端末１５３に置き換え、ＩＣカード５０２をＩＣカード５０９に置き換え、電子情報登録手段１２０を電子情報登録手段１６１に置き換え、電子情報復元手段１２１を電子情報復元手段１６２に置き換え、さらに、電子金庫

手段１１３を電子金庫手段１６４に置き換え、電子金庫手段１２３を電子金庫手段１６５に置き換えて、２つの電子金庫手段１６４と１６５とを通信回線で接続したものである。さらに、端末１６３に、実施例９（図１６）に示された所有者情報入力手段１４５、所有者認証情報保管手段１４８、所有者認証手段１４９を接続したものである。

以下、本実施例１２の動作について説明するが、基本的な動作は上記実施例３および９と同様であるので、以下にはこれらの実施例と異なる部分についてのみ説明する。所有者情報入力手段１４５、所有者認証情報保管手段１４８、所有者認証手段１４９を用いて、復号鍵を登録した別の電子金庫手段１６５に対する所有者認証が成功したとき、この別の電子金庫手段１６５が電子価値情報を登録した電子金庫手段１６４と通信を行って暗号化電子情報を取得する。端末１６３は、別の電子金庫手段１６５から暗号化電子情報を取得して、電子情報復元手段１６２に送る。電子情報復元手段１６２は、暗号化電子価値情報を復号して電子財布手段１０１上に復元する。一方、暗復号化手段１０５が、新しい暗号鍵と復号鍵の鍵ペアを生成し、この新しい暗号鍵を用いて電子財布手段１０１上の電子価値情報を再度暗号化し、電子情報登録手段１６１が、この新暗号化電子価値情報を電子金庫手段１６４に端末１６３を経由して送って登録証を取得するとともに、新しい復号鍵を別の電子金庫手段１６５に送って同様に登録証を取得する。

このように、本実施例１２では、安全のために電子価値情報と復号鍵を別別の電子金庫手段に預けた場合に、復号鍵を紛失した時や端末が破壊された時には、認証によって正当な情報保持者と認定されることを条件に、電子金庫手段同士が通信を行なって、電子価値情報と復号鍵とを合わせて端末に送り返してくるので、電子価値情報を復元することができる。また、電子価値情報を直ぐに利用しない場合は、新たな暗号鍵を用いて電子価値情報を暗号化し、それを一方の電子金庫手段に送るとともに、復号鍵を他方の電子金庫手段に送ることにより、従前の状態に戻すことができる。

以上説明した各実施例において、電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時、または新規の電子価値情報を電

子財布手段上に登録する時に、復元に十分な容量が電子財布記憶手段上に残っていない場合、容量不足をユーザに対して提示して復元作業を中断することができる。

また、上記各実施例において、電子情報登録手段が、電子財布手段から取得した電子価値情報を電子金庫手段に登録して対応する登録証を取得し、登録証が電子財布手段に正常に登録された時は、電子情報登録手段が、電子財布手段から電子価値情報を削除する。また、電子情報復元手段が、電子財布手段から取得した登録証を提示して電子金庫手段から対応する電子価値情報を取得し、電子価値情報を電子財布手段上に正常に復元した時は、電子情報復元手段が、電子財布手段から登録証を削除するとともに、電子金庫手段から電子価値情報を削除する。

また、上記各実施例において、バックアップを行うための起動トリガを、携帯端末を充電台に置いた時、携帯端末が所定時間使用されていない時、携帯端末のバッテリー容量が所定値以下に落ちた時、または所定時間毎、例えば携帯端末を使用していない夜中の２３時、またはＩＣカードのメモリー容量が所定値以下に落ちた時、または電子価値情報の利用可能期限、例えば１週間以上先の電子価値情報をバックアップする、等を基準にかけることにより、効率のよいバックアップを行うことができる。

また、バックアップから復元するための起動トリガを、携帯端末の電波受信状態が改善された時、携帯端末のバッテリー容量が所定値以上に回復した時、または所定時間毎、例えば携帯端末を使用可能な毎朝６時、またはＩＣカードのメモリー容量が所定値以上に回復した時、または電子価値情報の利用可能期限、例えば明日から使用可能な電子価値情報を今日復元する、等を基準にかけることにより、効率のよいバックアップ復元を行うことができる。

また、上記各実施例に記載した電子財布手段、電子金庫手段、電子情報登録手段、電子情報復元手段等の制御プログラムをソフトウェアで実現して、磁気ディスク、光磁気ディスク、ＲＯＭ、ＤＶＲＯＭなどの記録媒体に記録することにより、電子計算機による読み取りが可能になる。

請 求 の 範 囲

1. 電子価値情報を管理する電子財布手段と、

前記電子財布手段固有の記憶領域である電子財布記憶手段と、

電子価値情報の登録を受け付けて登録証を生成して発行し、前記登録証の提示によって対応する前記電子価値情報を取り出すことができる電子金庫手段と、

前記登録証に対応づけて前記電子価値情報を保持する電子金庫手段固有の記憶領域である電子金庫記憶手段と、

前記電子金庫手段に前記電子価値情報を登録して前記登録証を取得する電子情報登録手段と、

前記電子金庫手段に前記登録証を提示して前記電子価値情報を取得する電子情報復元手段とを備え、

前記電子情報登録手段が、前記電子財布手段より取得した電子価値情報を前記電子金庫手段に登録して対応する前記登録証を取得し、前記登録証を前記電子財布手段に登録することと、

前記電子情報復元手段が、前記電子財布手段より取得した前記登録証を前記電子金庫手段に提示して対応する前記電子価値情報を取得し、前記電子財布手段上に復元することを特徴とする電子情報バックアップシステム。

2. 前記電子金庫手段が、登録を要求された電子価値情報の部分情報を含んだ登録証を生成することを特徴とする請求項1に記載の電子情報バックアップシステム。

3. 前記電子金庫手段が、自分自身に対するポインタ情報を含んだ登録証を生成することによって、複数の電子金庫手段に対して電子価値情報の登録を可能としたことを特徴とする請求項1に記載の電子情報バックアップシステム。

4. 暗号鍵と復号鍵の組を保持する鍵保管手段と、前記電子価値情報に対し暗号鍵を用いた暗号化と前記復号鍵を用いた復号化を行う暗復号化手段とを備え、前記電子情報登録手段が、前記電子財布手段から取得した電子価値情報を前記暗復号化手段によって暗号化した暗号化電子価値情報を前記電子金庫手段に登録して暗号化電子価値情報登録証を取得することと、前記電子情報復元手段が、前記

暗号化電子価値情報登録証を前記電子金庫手段に提示して対応する前記暗号化電子価値情報を取得し、前記暗復号化手段によって復号化して前記電子価値情報を取得して前記電子金庫手段上に復元することを特徴とする請求項1から3のいずれかに記載の電子情報バックアップシステム。

5. 前記電子情報登録手段が、前記鍵保管手段から鍵情報を取得して前記電子金庫手段に登録して鍵登録証を取得することと、前記電子情報復元手段が、前記鍵登録証を前記電子金庫手段に提示して対応する前記鍵情報を取得し、前記取得した鍵情報を前記鍵保管手段上に復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

6. 前記暗号化した電子価値情報を復号化する復号鍵を、前記電子金庫手段とは別の電子金庫手段に登録して鍵登録証を取得することと、前記電子情報復元手段が、前記鍵登録証を前記別の電子金庫手段に提示して対応する前記鍵情報を取得し、前記取得した鍵情報を前記鍵保管手段上に復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

7. 前記電子価値情報を元の電子価値情報へ復元するための識別子を付加した任意の数の部分電子情報に分割する電子情報分割手段と、前記分割電子情報から元の前記電子価値情報を復元する電子情報合成手段とを備え、前記電子情報登録手段が、前記電子価値情報の分割を前記電子情報分割手段に要求して複数の部分電子情報を取得するとともに、前記部分電子情報の全てまたは一部を電子金庫手段に登録してそれぞれについての部分情報登録証を取得することと、前記電子情報復元手段が、前記部分情報登録証の全てまたは一部をそれぞれの部分情報登録証を発行した電子金庫手段に提示してそれぞれ対応する部分電子情報を取得することと、前記電子情報合成手段が、前記取得した部分電子情報から前記電子価値情報を復元することを特徴とする請求項4に記載の電子情報バックアップシステム。

8. 電子情報登録手段が、電子情報分割手段により分割された複数の分割電子情報をそれぞれ暗復号化手段を用いて暗号化して複数の暗号化分割電子情報を取得し、前記取得した複数の暗号化分割電子情報の全てまたは一部を電子金庫手

段に登録して対応する登録証を取得することを特徴とする請求項７に記載の電子情報バックアップシステム。

９．　電子情報登録手段が、電子価値情報を前記暗復号化手段を用いて暗号化して暗号化電子情報を取得し、前記取得した暗号化電子情報を前記電子情報分割手段を用いて複数の分割暗号化電子情報を取得するとともに、前記複数の分割暗号化電子情報の全てまたは一部を電子金庫手段に登録して対応する登録証を取得することを特徴とする請求項７に記載の電子情報バックアップシステム。

１０．　複数の電子価値情報を結合して一つの結合電子情報として出力する電子情報結合手段と、前記結合電子情報を元の複数の電子情報に分割する電子情報結合解除手段とを備え、前記電子情報結合手段が、複数の電子価値情報の組から結合電子情報を生成することと、前記電子情報登録手段が、前記結合電子情報を前記電子金庫手段に登録して対応する結合電子情報登録証を取得することと、前記電子情報復元手段が、前記結合電子情報登録証を提示して電子金庫手段から対応する結合電子情報を取得することと、前記電子情報結合解除手段が、前記結合電子情報から前記電子価値情報の組を取得することを特徴とする請求項７に記載の電子情報バックアップシステム。

１１．　前記電子情報分割手段が、前記電子情報登録手段が前記鍵保管手段から取得した鍵情報を複数の部分鍵に分割することと、前記暗復号化手段が、前記電子情報登録手段が前記電子財布手段から取得した電子価値情報を暗号化して暗号化電子情報を取得することと、前記電子情報結合手段が、前記暗号化電子情報と前記部分鍵の一部である部分鍵群Ａとから結合電子情報を取得することと、前記電子情報登録手段が、前記結合電子情報と残りの部分鍵である部分鍵群Ｂとをそれぞれ異なる電子金庫手段に登録して対応する登録証を取得することと、前記電子情報復元手段が、前記登録証を対応する前記電子金庫手段に提示して前記結合電子情報と前記部分鍵群Ｂとを取得することと、前記電子情報結合解除手段が、前記結合電子情報を前記暗号化電子情報と前記部分鍵群Ａとに分離することと、前記電子情報合成手段が、前記部分鍵群Ａと前記部分鍵群Ｂとを合成して鍵情報を生成することと、前記暗複合化手段が、前記暗号化電子情報を復号して前記電

子価値情報を取得することと、前記電子情報復元手段が、前記鍵情報を取得して前記鍵保管手段上に復元するとともに、前記電子価値情報を電子財布手段上に復元することを特徴とする請求項１０に記載の電子情報バックアップシステム。

１２．　前記電子情報分割手段が、鍵情報を分割して得る部分鍵を暗号鍵と復号鍵の鍵ペアを生成する元となる情報とすることを特徴とする請求項１１に記載の電子情報バックアップシステム。

１３．　復号鍵を生成するために用いる元の暗号種（たね）情報と、前記暗号種情報から復号鍵を生成する復号鍵生成アルゴリズムとを備え、前記電子情報登録手段が、前記暗号種情報を前記電子金庫手段に登録して対応する暗号種情報登録証を取得することと、前記電子情報復元手段が、前記暗号種情報登録証を提示して前記電子金庫手段から対応する暗号種情報を取得することと、前記暗復号化手段が、前記暗号種情報に前記復号鍵生成アルゴリズムをかけて復号鍵を生成するとともに、前記電子情報復元手段が取得した前記電子価値情報を前記復号鍵を用いて復号化することを特徴とする請求項４、６、７、１０、１１のいずれかに記載の電子情報バックアップシステム。

１４．　所有者固有の所有者情報を入力する所有者情報入力手段と、
前記所有者情報に対応する所有者認証情報を入力する所有者認証情報入力手段とを備え、前記電子情報登録手段が、前記電子価値情報と前記所有者認証情報入力手段より取得した所有者認証情報とを組として前記電子金庫手段に登録することと、前記電子情報復元手段が、前記所有者情報入力手段より取得した所有者情報を前記電子金庫手段に提示して前記所有者認証情報と照合が成功した時に、前記電子価値情報を取得できることを特徴とする請求項１、４、６、７、１０、１１のいずれかに記載の電子情報バックアップシステム。

１５．　所有者固有の所有者情報を入力する所有者情報入力手段と、
前記所有者情報に対応する所有者認証情報を保持する所有者認証情報保管手段と、前記所有者情報と前記所有者認証情報とを対照して正当性を検証する所有者認証手段とを備え、前記所有者情報入力手段から入力された所有者情報を前記所有者認証手段に提示して認証を行うことと、その認証結果を用いて前記電子情報登録

手段と電子金庫手段との間の暗号化通信路を構築することと、前記暗号化通信路を通して前記電子情報登録手段が前記電子価値情報を電子金庫手段に登録することと、前記電子金庫手段が前記認証結果に対応する所有者認証情報と前記電子価値情報とを組として電子金庫記憶手段に保持することと、前記電子情報復元手段が前記暗号化通信路を通して前記認証結果に対応する前記所有者認証情報に対応する前記電子価値情報を取得することを特徴とする請求項１、４、６、７、１０、１１のいずれかに記載の電子情報バックアップシステム。

１６．　前記所有者情報入力手段と所有者認証手段が一時的に利用する共通鍵を生成し共有することと、前記共通鍵によって所有者情報を暗号化して所有者認証手段に送信することを特徴とする請求項１５に記載の電子情報バックアップシステム。

１７．　前記所有者情報入力手段が所有者認証手段固有の秘密鍵に対応した公開鍵で所有者情報を暗号化することと、前記所有者情報入力手段が前記の暗号化した所有者情報を所有者認証手段に送信することを特徴とする請求項１６に記載の電子情報バックアップシステム。

１８．　所有者認証に用いる認証機器を読み取る認証機器読み取り手段と、前記認証機器の正当性を検証する認証確認手段と、前記認証確認手段が前記認証機器の正当性確認で対照する情報を保持する認証確認情報保管手段とを備え、前記認証機器読み取り手段に接続された認証機器と認証確認手段が相互に正当性を確認することを特徴とする請求項１、４、６、７、１０、１１のいずれかに記載の電子情報バックアップシステム。

１９．　所有者認証に用いる認証機器を読み取る認証機器読み取り手段と、前記認証機器の正当性を検証する認証確認手段と、前記認証確認手段が前記認証機器の正当性確認で対照する情報を保持する認証確認情報保管手段とを備え、前記認証機器読み取り手段に接続された認証機器と認証確認手段が相互に正当性を確認することと、その認証結果を用いて電子情報登録手段と電子金庫手段の間の暗号化通信路を構築することと、前記暗号化通信路を通して電子情報登録手段が電子価値情報を電子金庫手段に登録することと、前記電子金庫手段が前記認証結果

に対応する所有者認証情報と前記電子価値情報とを組として電子金庫記憶手段に保持することと、前記電子情報復元手段が前記暗号化通信路を通して前記認証結果に対応する前記所有者認証情報に対応する前記電子価値情報を取得することを特徴とする請求項１、４、６、７、１０、１１のいずれかに記載の電子情報バックアップシステム。

２０．　電子価値情報をバックアップする条件情報を保持するバックアップ条件保管手段と、前記バックアップ条件保管手段から取得したバックアップ条件を解釈して前記電子財布手段からバックアップ対象を選択するバックアップ対象抽出手段とを備え、前記電子情報登録手段が前記バックアップ対象の電子価値情報を自動的に前記電子金庫手段に登録して対応する登録証を取得することを特徴とする請求項１、４、６、７、１０、１１、１４、１５、１８、１９のいずれかに記載の電子情報バックアップシステム。

２１．　電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時または新規の電子価値情報を電子財布手段上に登録する時に復元に十分な容量が電子財布記憶手段上に残っていない場合、電子情報登録手段が前記バックアップ対象抽出手段を用いて前記電子財布手段上からバックアップ対象の電子価値情報を選択して前記電子財布金庫手段に登録して対応する登録証を取得することと、前記バックアップ対象の電子価値情報を前記電子財布記憶手段上から削除して空き容量を拡大することと、空き容量を確保が完了した時に前記の電子財布手段上への電子情報の復元または新規登録を継続することを特徴とした請求項２０に記載の電子情報バックアップシステム。

２２．　前記復号鍵を登録した別の電子金庫手段への所有者認証が成功したとき、前記別の電子金庫手段が前記復号鍵以外の電子価値情報を登録した電子金庫手段と通信を行って暗号化電子情報を取得することと、前記電子情報復元手段が前記別の電子金庫手段から前記暗号化された電子価値情報を取得して前記電子財布手段上に復元することを特徴とする請求項６に記載の電子情報バックアップシステム。

２３．　前記復号鍵を登録した別の電子金庫手段への所有者認証が成功したと

き、前記別の電子金庫手段が前記復号鍵以外の電子価値情報を登録した電子金庫手段と通信を行って暗号化電子情報を取得することと、前記電子情報復元手段が前記別の電子金庫手段から前記暗号化された電子価値情報を取得して前記電子財布手段上に復元することと、前記暗復号化手段が新しい暗号鍵と復号鍵の鍵ペアを生成することと、前記新しい暗号鍵を用いて前記電子価値情報を暗号化して、前記新暗号化電子価値情報を前記電子金庫手段に送るとともに、前記新しい復号鍵を前記別の電子金庫手段に送ることを特徴とする請求項６に記載の電子情報バックアップシステム。

２４．　前記電子情報復元手段が登録証を提示して対応する電子価値情報を電子財布手段上に復元する時、または新規の電子価値情報を電子財布手段上に登録する時に、復元に十分な容量が電子財布記憶手段上に残っていない場合、容量不足をユーザに対して提示して復元作業を中断することを特徴とした請求項１から２３のいずれかに記載の電子情報バックアップシステム。

２５．　前記電子情報登録手段が、前記電子財布手段から取得した電子価値情報を前記電子金庫手段に登録して対応する登録証を取得し、前記登録証が前記電子財布手段に正常に登録された時は、前記電子情報登録手段が、前記電子財布手段から前記電子価値情報を削除することを特徴とする請求項１から２４のいずれかに記載の電子情報バックアップシステム。

２６．　前記電子情報復元手段が、前記電子財布手段から取得した登録証を提示して前記電子金庫手段から対応する電子価値情報を取得し、前記電子価値情報を電子財布手段上に正常に復元した時は、前記電子情報復元手段が、前記電子財布手段から前記登録証を削除するとともに、前記電子金庫手段から前記電子価値情報を削除することを特徴とする請求項１から２５のいずれかに記載の電子情報バックアップシステム。

２７．　電子価値情報を外部サーバに登録してその登録証を取得するとともに、前記電子価値情報および登録証を記憶媒体に記憶し、前記外部サーバ対して登録証を提示して電子価値情報を復元するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

２８．　前記登録証に電子価値情報の部分情報を含むことを特徴とする請求項２７に記載の電子情報バックアップシステム。

２９．　登録要求された電子価値情報を暗号鍵を用いて暗号化して暗号化電子価値情報を取得するとともに、前記暗号化電子価値情報を外部サーバに登録するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

３０．　復元要求された登録証を外部サーバに提示して対応する暗号化電子価値情報を取得し、前記暗号化電子価値情報を復号鍵を用いて電子価値情報に復元するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

３１．　登録要求された電子価値情報を分割して複数の部分電子情報を取得し、前記部分電子情報のすべてを任意の数の外部サーバに登録して前記部分電子情報と同数の部分情報登録証を取得するとともに、前記部分情報登録証のすべてを記憶媒体に記憶するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

３２．　前記すべての部分情報登録証を外部サーバに提示して同数の部分電子情報を取得し、前記部分電子情報のすべてを合成して元の電子価値情報を復元して前記記憶媒体に記憶することを特徴とする請求項３１に記載の電子情報バックアップシステム。

３３．　電子価値情報を復号鍵に対応した暗号鍵で暗号化して暗号化電子価値情報を取得し、前記復号鍵を分割して複数の部分復号鍵とし、前記部分復号鍵の一以上と前記暗号化電子価値情報とを結合して結合電子情報を取得し、前記結合電子情報を外部サーバに登録して結合登録証を取得し、残りの部分復号鍵を別の外部サーバに登録し、前記結合登録証を記憶媒体に記憶するバックアップ手段を備えたことを特徴とする電子情報バックアップシステム。

３４．　前記結合登録証を前記外部サーバに提示して前記結合電子情報を取得し、前記結合電子情報を結合解除して前記暗号化電子価値情報と一以上の部分復号鍵に分解し、前記残りの部分復号鍵を前記別の外部サーバから取得し、前記分解した部分復号鍵と前記取得した部分復号鍵とを合成して元の復号鍵に復元し、前記復元した復号鍵を用いて前記暗号化電子価値情報を元の電子価値情報に復元

して前記記憶媒体に記憶することを特徴とする請求項３３に記載の電子情報バックアップシステム。

３５．　電子価値情報に対応する登録証を外部サーバから取得した時に、前記登録証に対応する前記電子価値情報を前記記憶媒体から削除することを特徴とする請求項２７から３４のいずれかに記載の電子情報バックアップシステム。

３６．　予め設定されたバックアップ条件を解釈して前記記憶媒体からバックアップ対象の電子価値情報を選択し、前記選択された電子価値情報を自動的に前記外部サーバに登録して対応する登録証を取得することを特徴とする請求項２７から３５のいずれかに記載の電子情報バックアップシステム。

３７．　認証用情報と電子価値情報とを組として前記外部サーバに登録することを特徴とする請求項２７から３６のいずれかに記載の電子情報バックアップシステム。

３８．　入力された所有者情報を前記外部サーバに提示して前記外部サーバに登録された認証用情報と一致した時に、前記電子価値情報を取得可能とすることを特徴とする請求項３７に記載の電子情報バックアップシステム。

３９．　入力された所有者情報に対応する所有者認証情報を記憶媒体に保持し、前記所有者情報と前記所有者認証情報とを照合して一致した時に、前記電子価値情報を取得可能とすることを特徴とする請求項２７から３６のいずれかに記載の電子情報バックアップシステム。

４０．　前記所有者情報と前記所有者認証情報とが一致した時に、前記外部サーバとの間に暗号化通信路を構築し、前記所有者情報に対応する電子価値情報を取得可能とすることを特徴とする請求項３９に記載の電子情報バックアップシステム。

４１．　所有者認証情報を記録したＩＣカードを読み取ってその認証情報を外部サーバに送り、前記外部サーバが前記認証情報の正当性を確認した時に、前記電子価値情報を取得可能とすることを特徴とする請求項２７から３６のいずれかに記載の電子情報バックアップシステム。

４２．　前記認証情報の正当性を確認した時に、前記外部サーバとの間に暗号

化通信路を構築し、前記認証情報に対応する電子価値情報を取得可能とすることを特徴とする請求項４１に記載の電子情報バックアップシステム。

４３．　復号鍵を登録した別の外部サーバへの所有者認証が成功した時に、前記別の外部サーバが前記復号鍵以外の電子価値情報を登録した外部サーバと通信を行って暗号化電子情報を取得して前記復号鍵と結合することを特徴とする請求項２７または３６のいずれかに記載の電子情報バックアップシステム。

４４．　前記暗号化電子情報を取得して復号した後、新たな暗号鍵を用いて前記電子価値情報を暗号化し、それを前記外部サーバに登録とともに、復号鍵を別の外部サーバに登録することを特徴とする請求項４３に記載の電子情報バックアップシステム。

図1

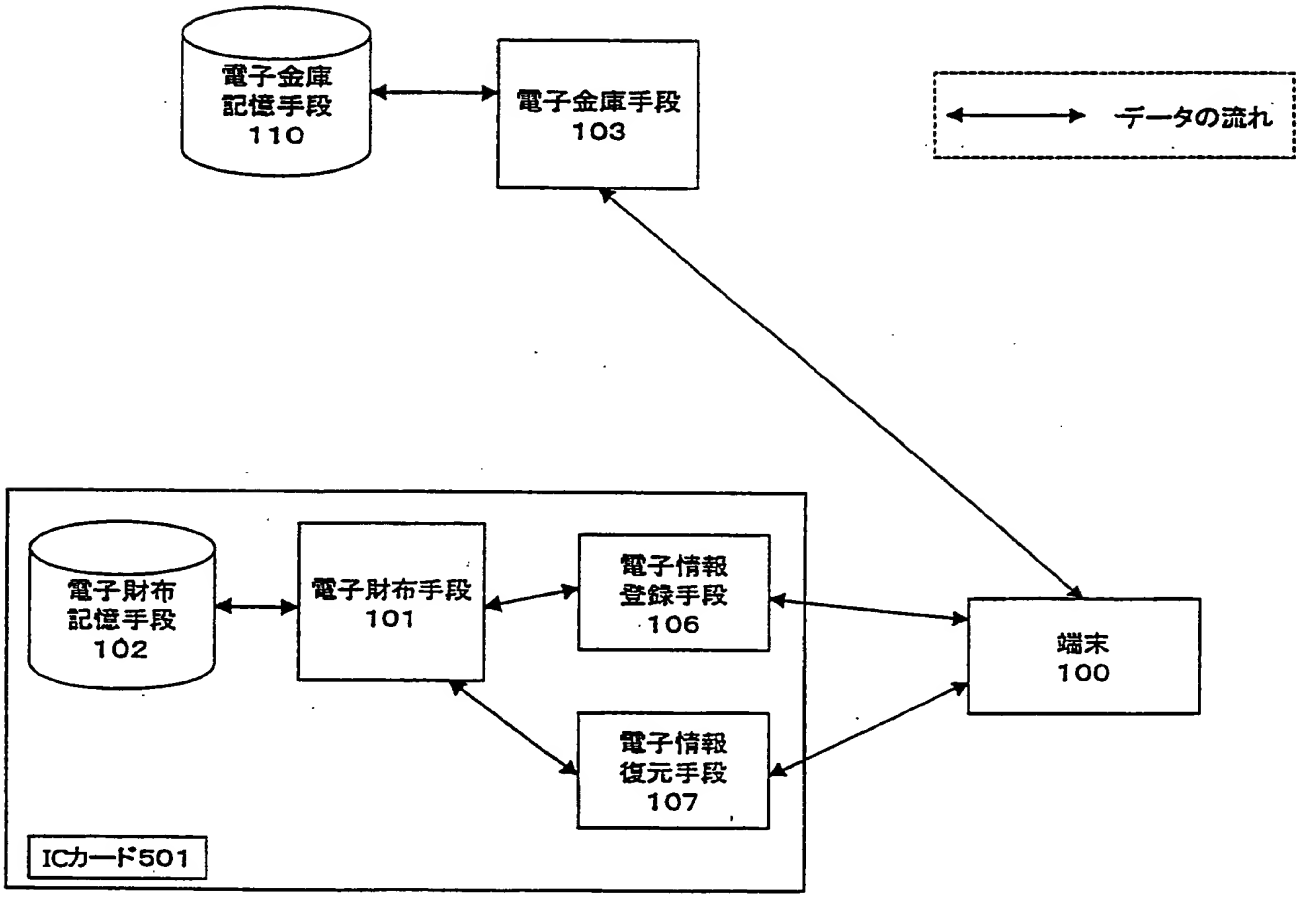

電子金庫
記憶手段
110
電子金庫手段
103
データの流れ
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
106
端末
100
電子情報
復元手段
107
ICカード501

図2

電子価値情報201

情報種別	映画チケット
名前	映画タイトル
単価	A円
数	B
合計金額	A×B円
場所	劇場名
有効期限	C～D
備考	……

(a)

ダイジェスト302

情報種別	映画チケット
名前	映画タイトル
数	B
有効期限	C～D
場所	劇場名

(b)

登録証301

ダイジェスト302	ハッシュ値X1	カウンタ値Y1

(c)

図3

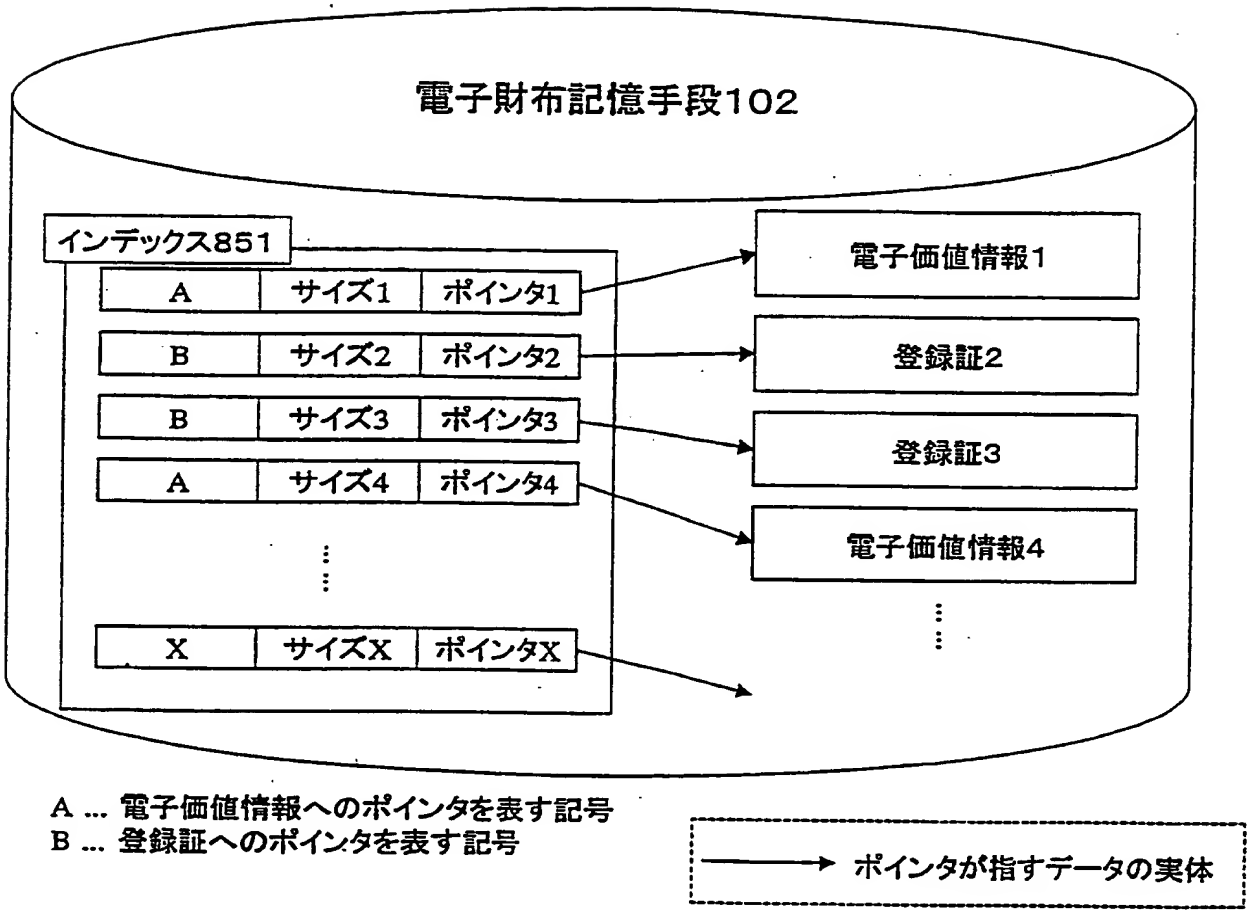
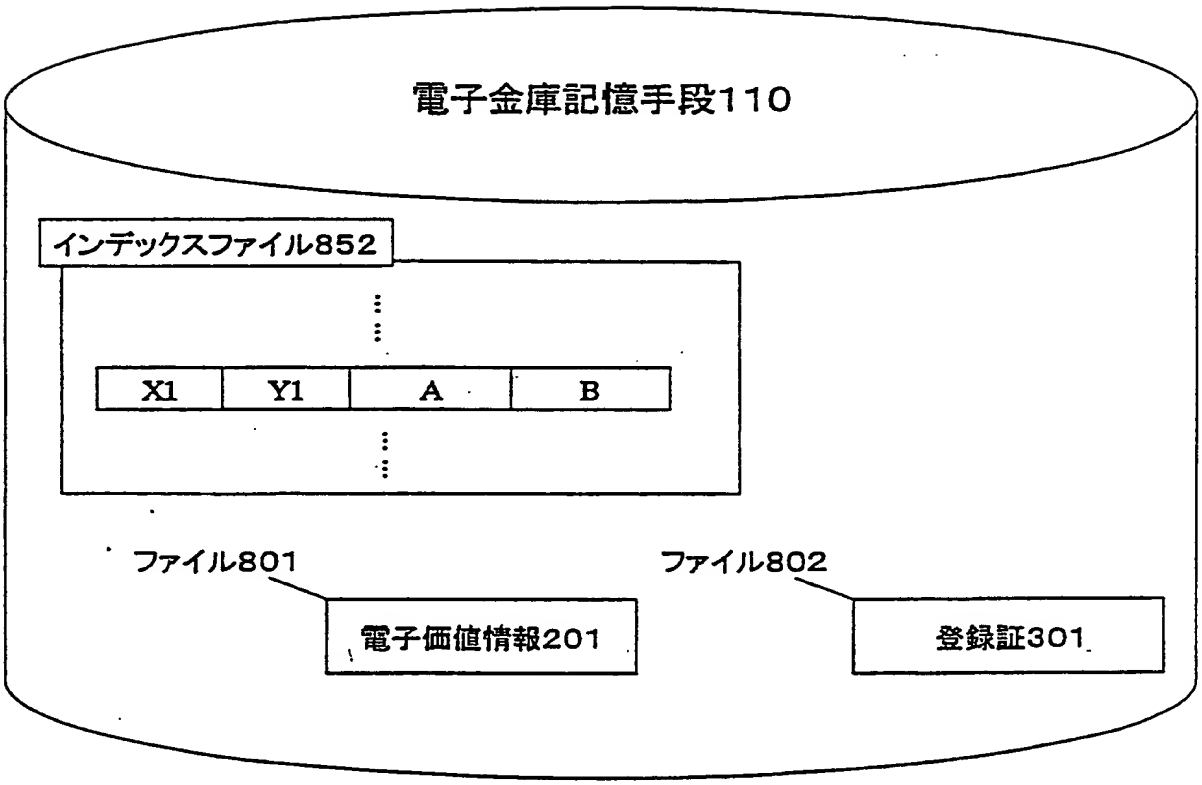

電子財布記憶手段102
インデックス851
A
サイズ1
ポインタ1
B
サイズ2
ポインタ2
B
サイズ3
ポインタ3
A
サイズ4
ポインタ4
X
サイズX
ポインタX
電子価値情報1
登録証2
登録証3
電子価値情報4
A ... 電子価値情報へのポインタを表す記号
B ... 登録証へのポインタを表す記号
ポインタが指すデータの実体

図4



A ... ファイル801のパス情報
B ... ファイル802のパス情報
X1 ... 登録証301の構成要素のハッシュ値
Y1 ... 登録証301の構成要素のカウンタ値

図5

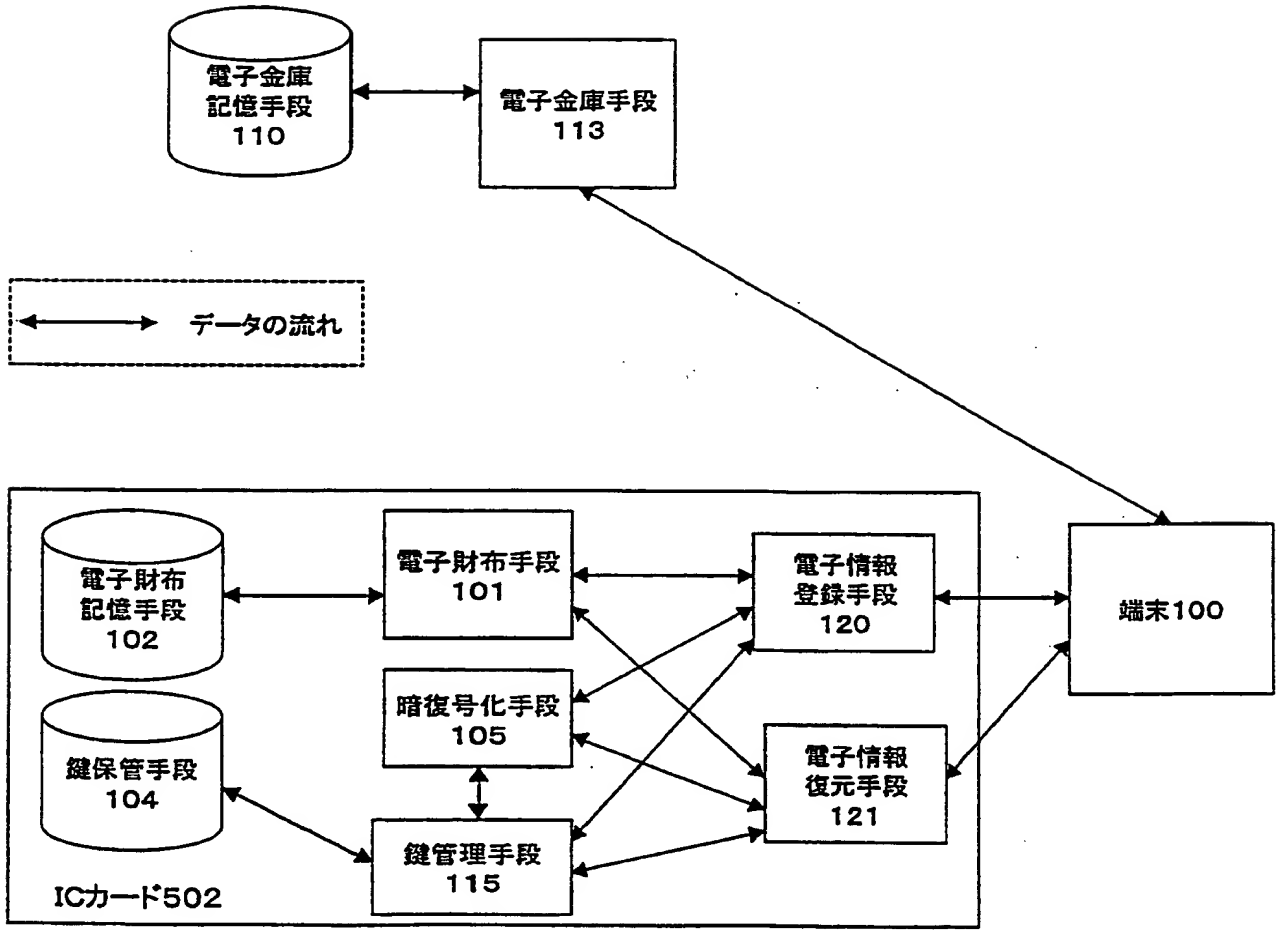

電子金庫
記憶手段
110
電子金庫手段
113
データの流れ
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
120
端末100
暗復号化手段
105
鍵保管手段
104
電子情報
復元手段
121
鍵管理手段
115
ICカード502

図6

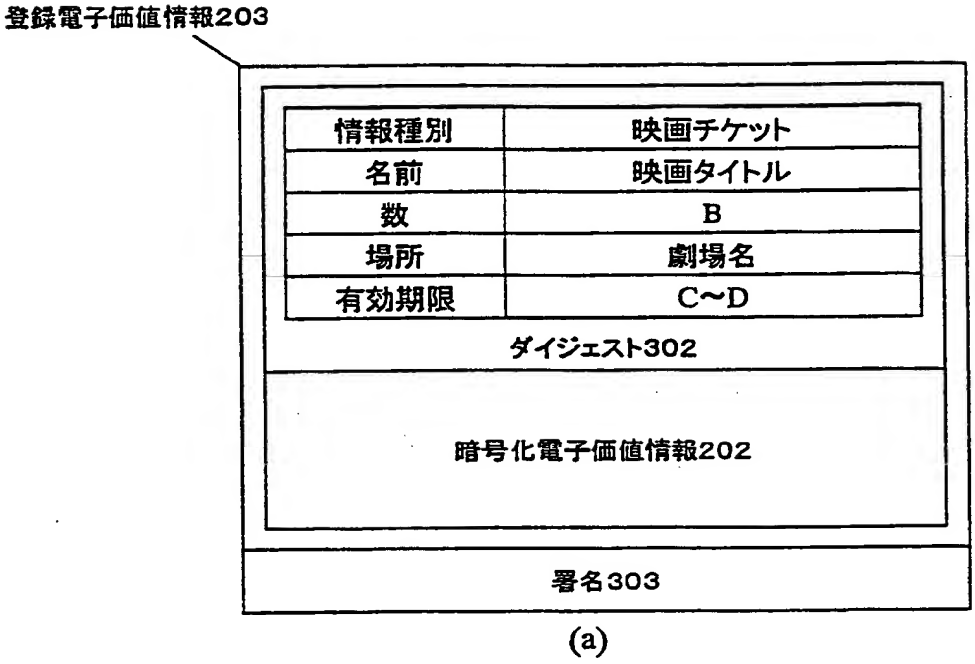

登録電子価値情報203
情報種別
映画チケット
名前
映画タイトル
数
B
場所
劇場名
有効期限
C～D
ダイジェスト302
暗号化電子価値情報202
署名303
(a)
登録証304
ダイジェスト302
ハッシュ値X2
カウンタ値Y2
(b)

図7

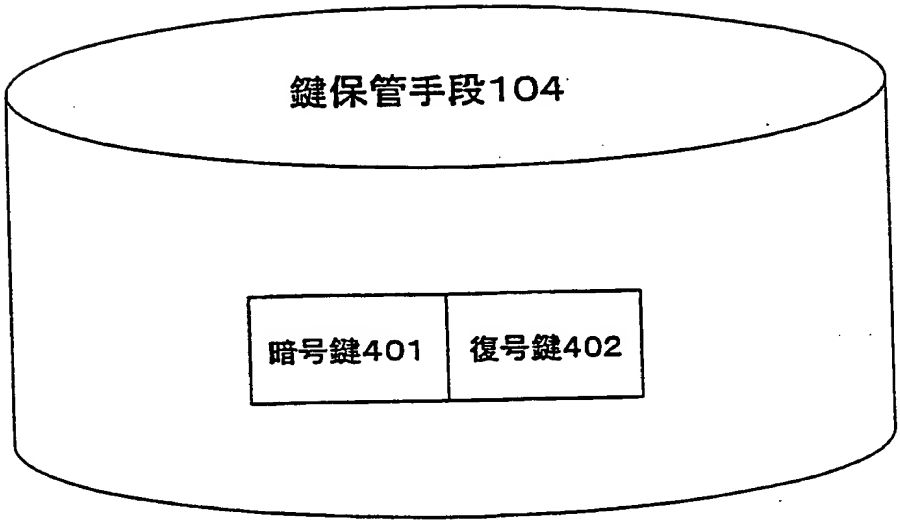
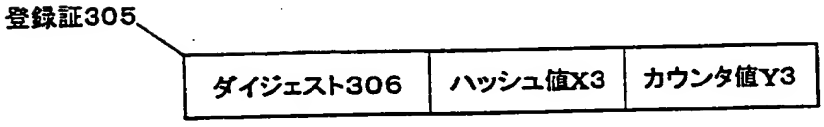
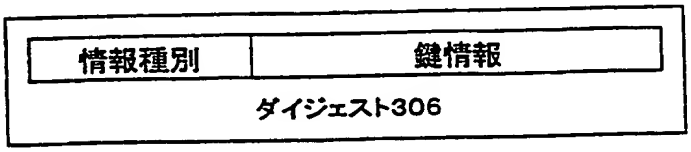

鍵保管手段104
暗号鍵401
復号鍵402

図8

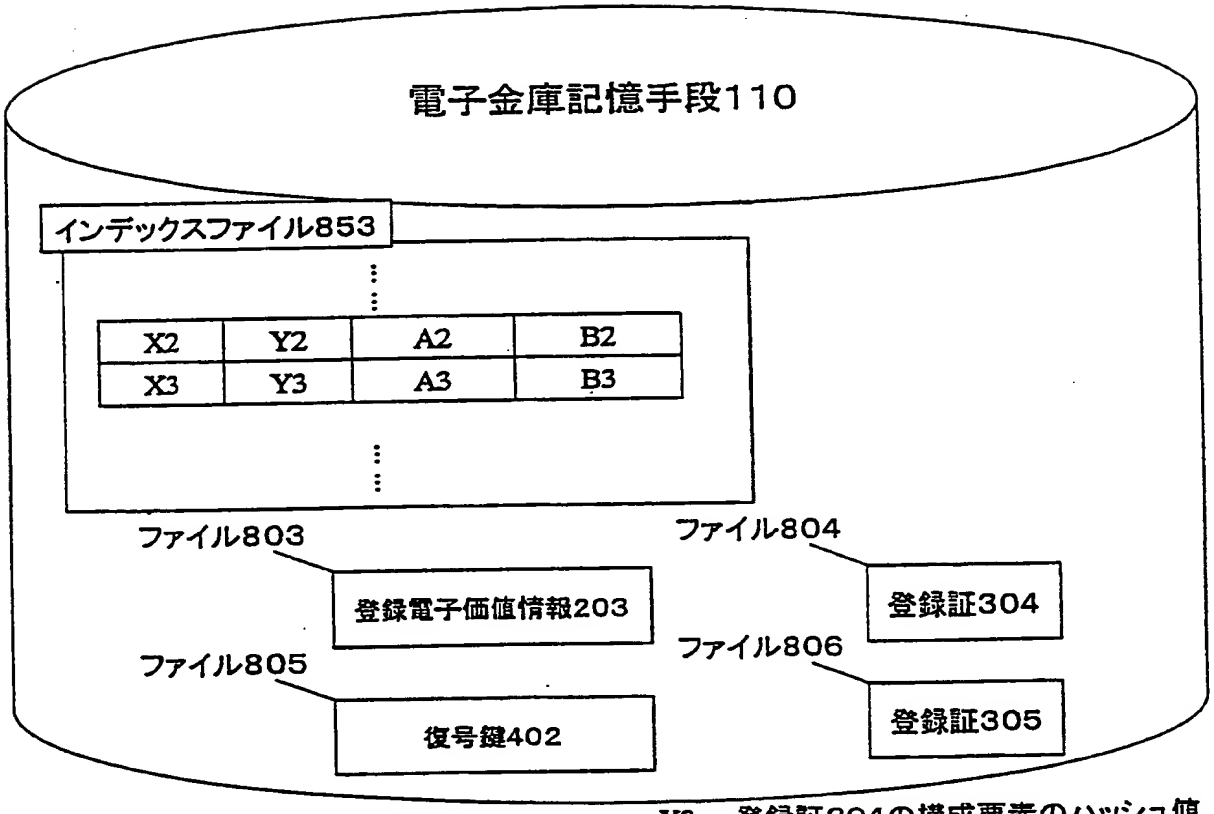

登録証305
ダイジェスト306
ハッシュ値X3
カウンタ値Y3

(a)


情報種別
鍵情報
ダイジェスト306

(b)

図9



A2 ... ファイル803のパス情報
B2 ... ファイル804のパス情報
A3 ... ファイル805のパス情報
B3 ... ファイル806のパス情報

X2 ... 登録証304の構成要素のハッシュ値
Y2 ... 登録証304の構成要素のカウンタ値
X3 ... 登録証305の構成要素のハッシュ値
Y3 ... 登録証305の構成要素のカウンタ値

図１０

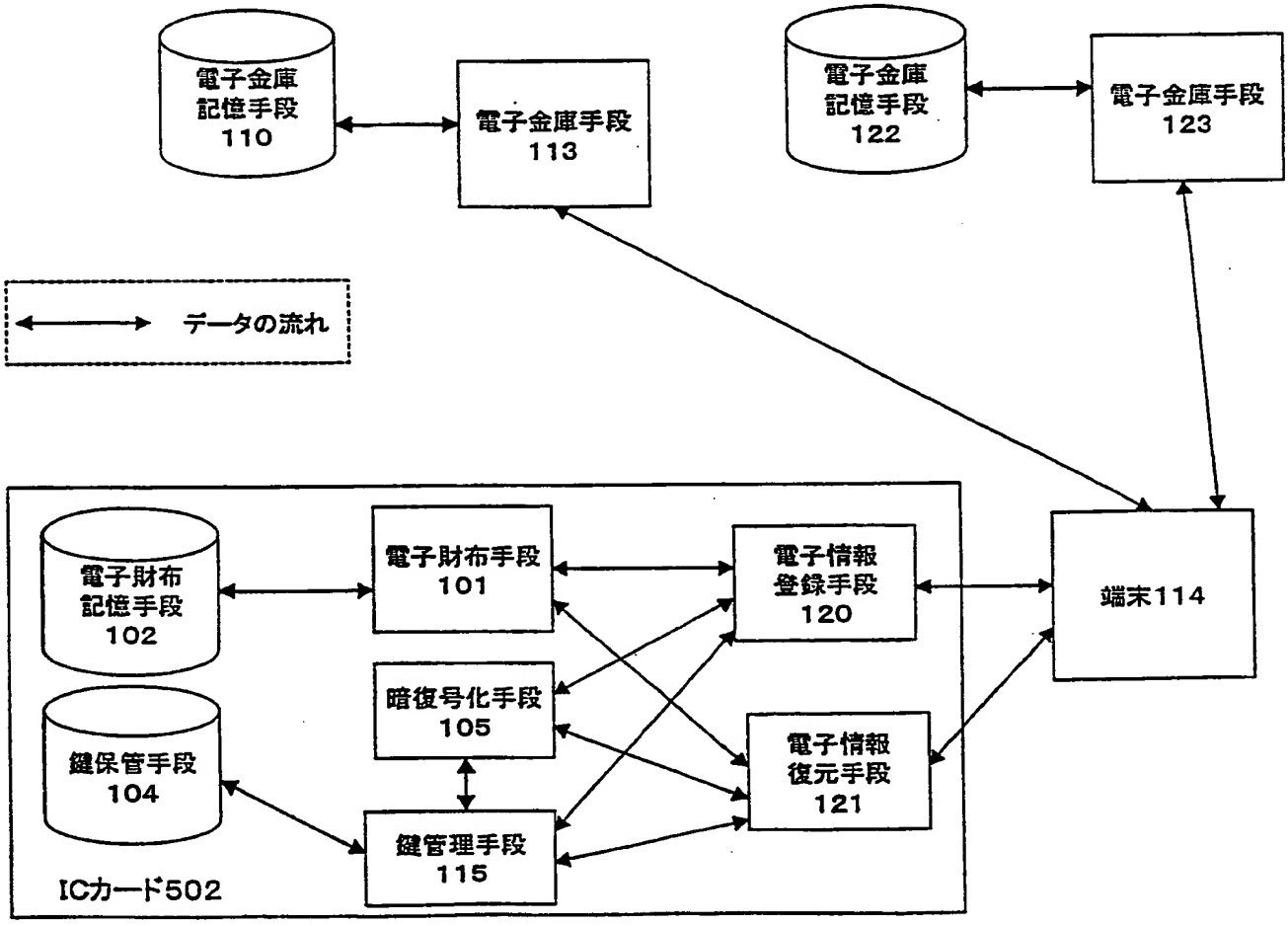

電子金庫
記憶手段
110
電子金庫手段
113
電子金庫
記憶手段
122
電子金庫手段
123
データの流れ
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
120
端末114
暗復号化手段
105
鍵保管手段
104
電子情報
復元手段
121
鍵管理手段
115
ICカード502

図11

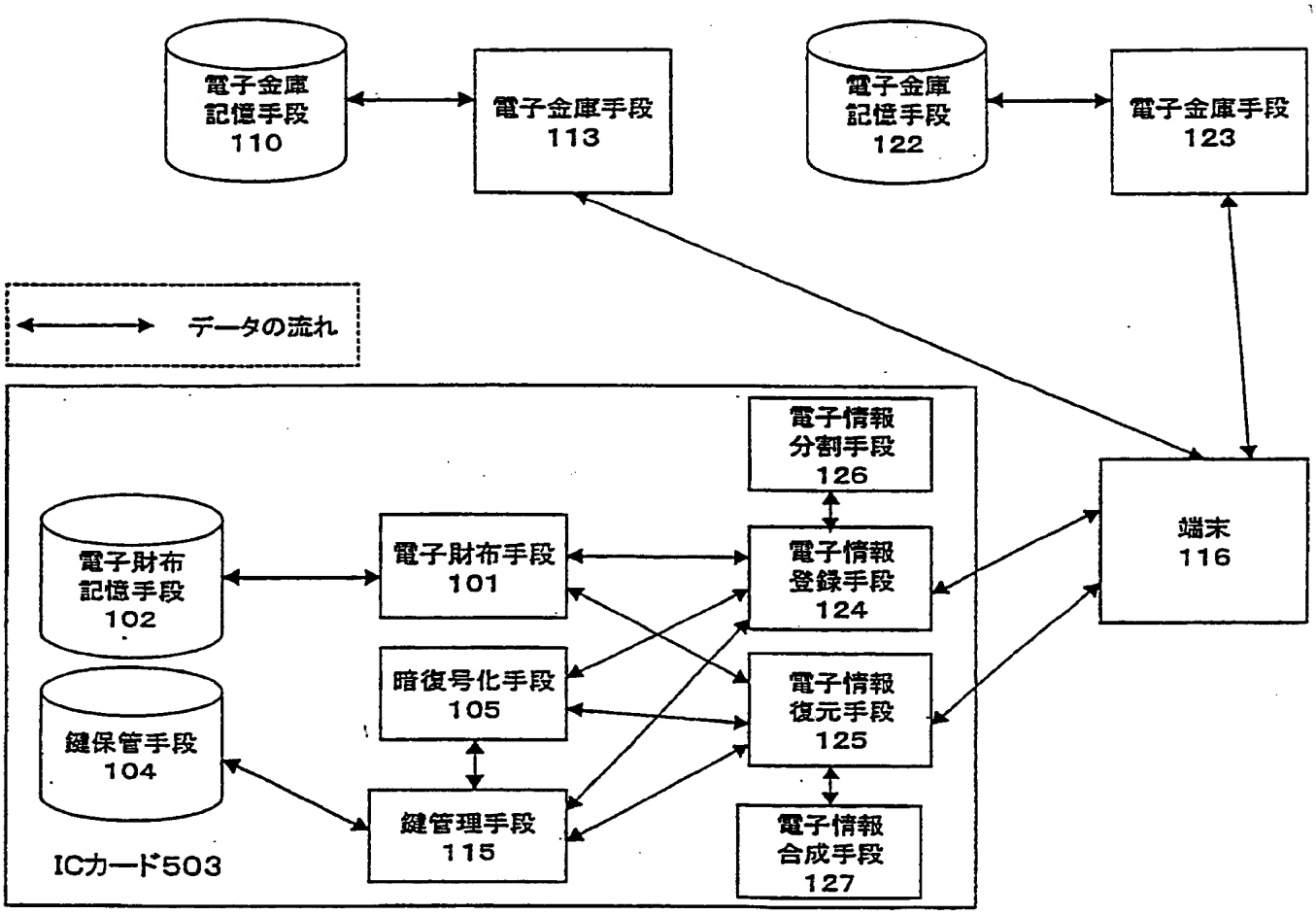

電子金庫
記憶手段
110
電子金庫手段
113
電子金庫
記憶手段
122
電子金庫手段
123
データの流れ
電子情報
分割手段
126
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
124
端末
116
暗復号化手段
105
電子情報
復元手段
125
鍵保管手段
104
鍵管理手段
115
電子情報
合成手段
127
ICカード503

図12

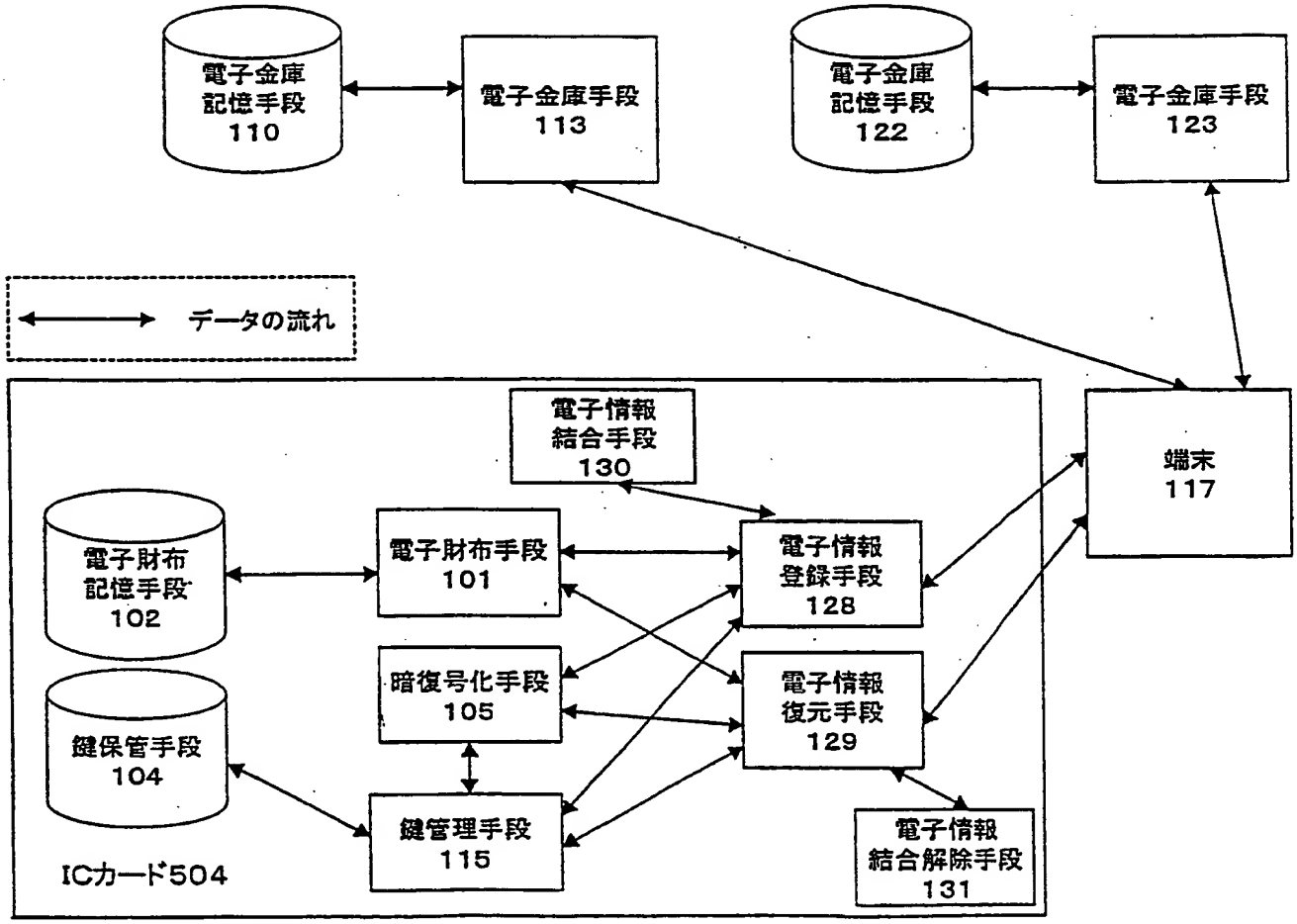

電子金庫
記憶手段
110
電子金庫手段
113
電子金庫
記憶手段
122
電子金庫手段
123
データの流れ
電子情報
結合手段
130
端末
117
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
128
暗復号化手段
105
電子情報
復元手段
129
鍵保管手段
104
鍵管理手段
115
電子情報
結合解除手段
131
ICカード504

図13

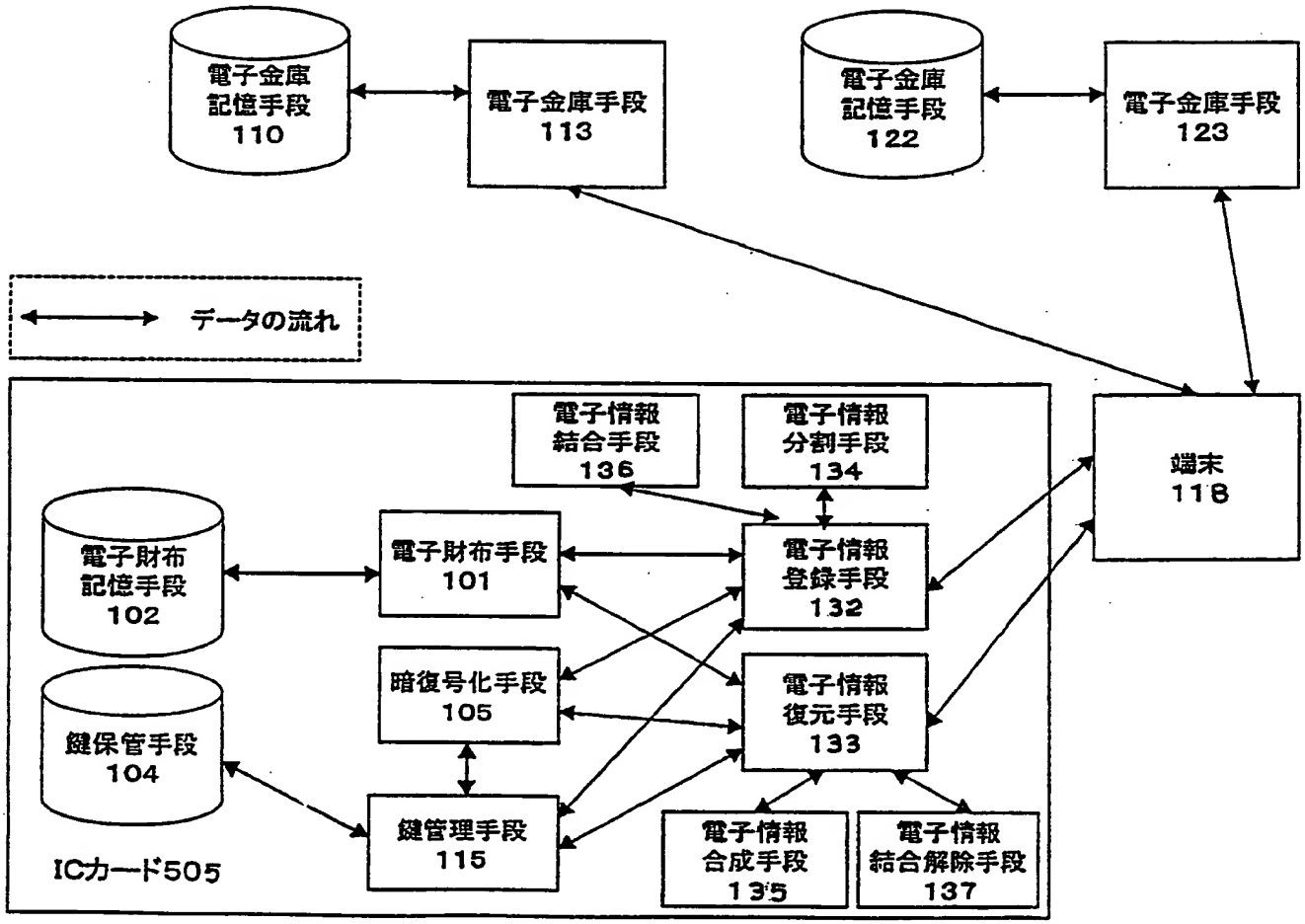

電子金庫
記憶手段
110
電子金庫手段
113
電子金庫
記憶手段
122
電子金庫手段
123
データの流れ
電子情報
結合手段
136
電子情報
分割手段
134
端末
118
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
132
暗復号化手段
105
電子情報
復元手段
133
鍵保管手段
104
鍵管理手段
115
電子情報
合成手段
135
電子情報
結合解除手段
137
ICカード505

図14

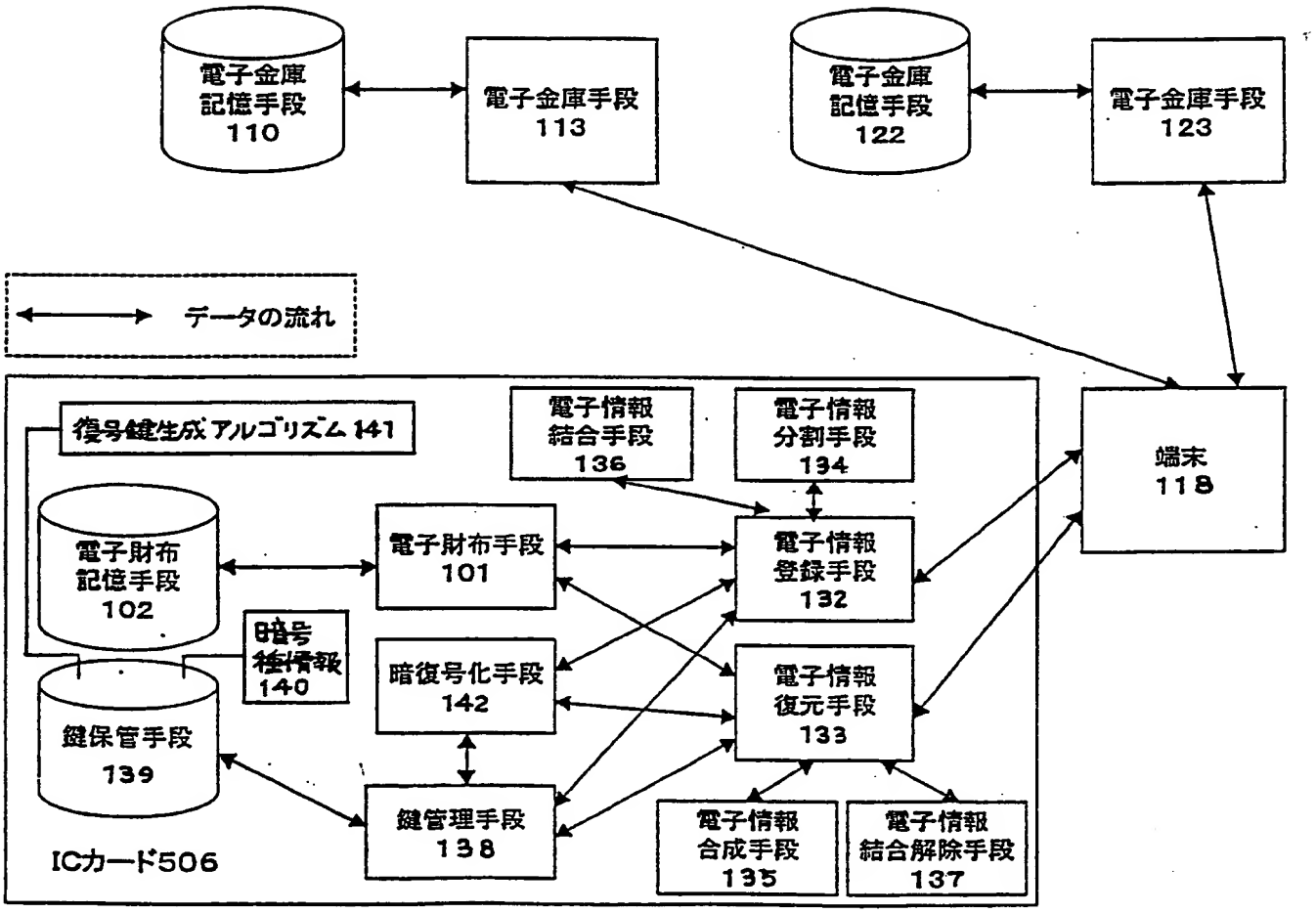

電子金庫
記憶手段
110
電子金庫手段
113
電子金庫
記憶手段
122
電子金庫手段
123
データの流れ
復号鍵生成アルゴリズム 141
電子情報
結合手段
136
電子情報
分割手段
134
端末
118
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
132
暗号
種情報
140
暗復号化手段
142
電子情報
復元手段
133
鍵保管手段
139
鍵管理手段
138
電子情報
合成手段
135
電子情報
結合解除手段
137
ICカード506

図15

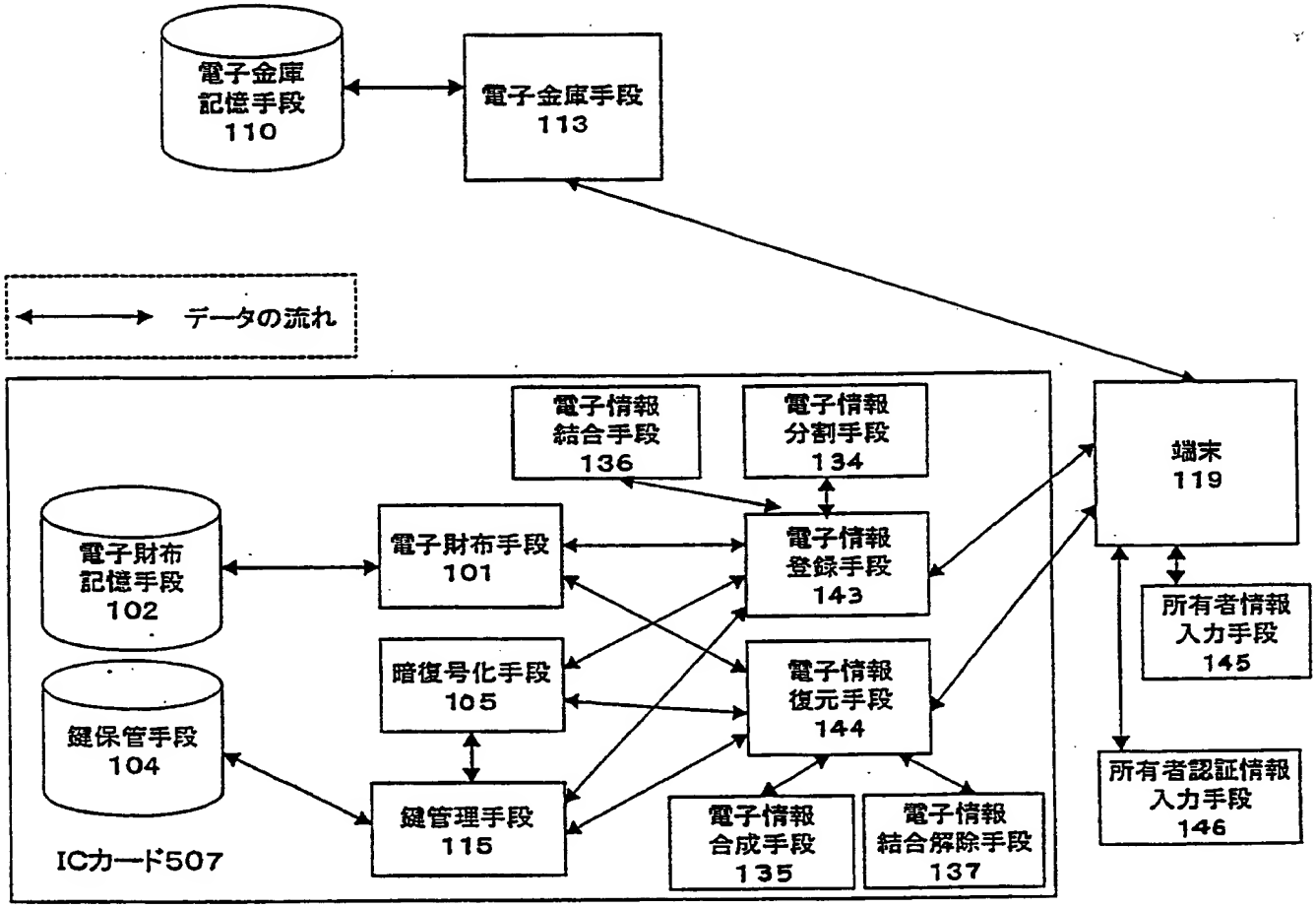

電子金庫
記憶手段
110
電子金庫手段
113
データの流れ
電子情報
結合手段
136
電子情報
分割手段
134
端末
119
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
143
所有者情報
入力手段
145
暗復号化手段
105
電子情報
復元手段
144
鍵保管手段
104
鍵管理手段
115
電子情報
合成手段
135
電子情報
結合解除手段
137
所有者認証情報
入力手段
146
ICカード507

図16

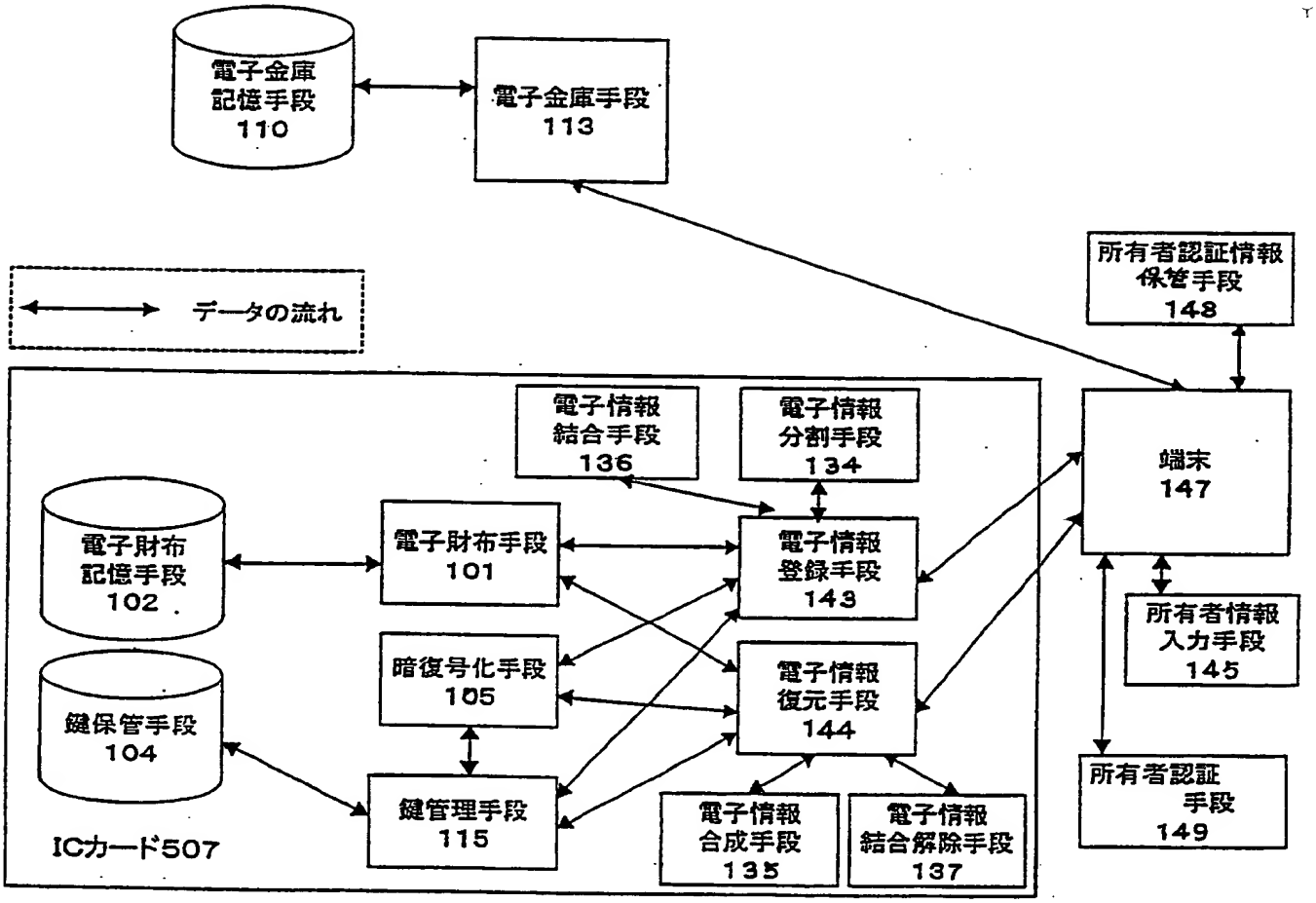

電子金庫
記憶手段
110
電子金庫手段
113
所有者認証情報
保管手段
148
データの流れ
電子情報
結合手段
136
電子情報
分割手段
134
端末
147
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
143
所有者情報
入力手段
145
暗復号化手段
105
電子情報
復元手段
144
鍵保管手段
104
鍵管理手段
115
所有者認証
手段
149
電子情報
合成手段
135
電子情報
結合解除手段
137
ICカード507

図17

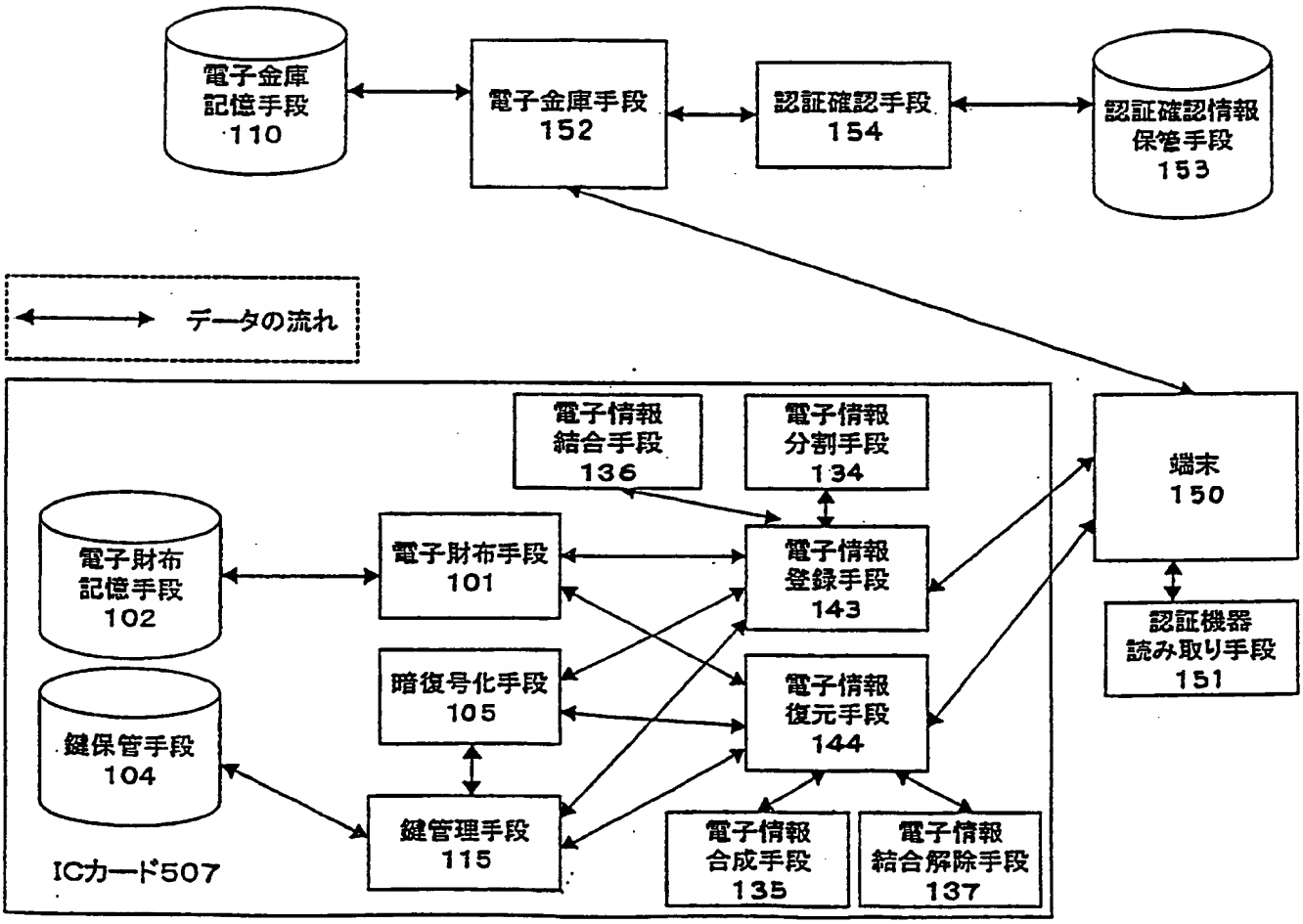

電子金庫
記憶手段
110
電子金庫手段
152
認証確認手段
154
認証確認情報
保管手段
153
データの流れ
電子情報
結合手段
136
電子情報
分割手段
134
端末
150
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
143
認証機器
読み取り手段
151
暗復号化手段
105
電子情報
復元手段
144
鍵保管手段
104
鍵管理手段
115
電子情報
合成手段
135
電子情報
結合解除手段
137
ICカード507

図18

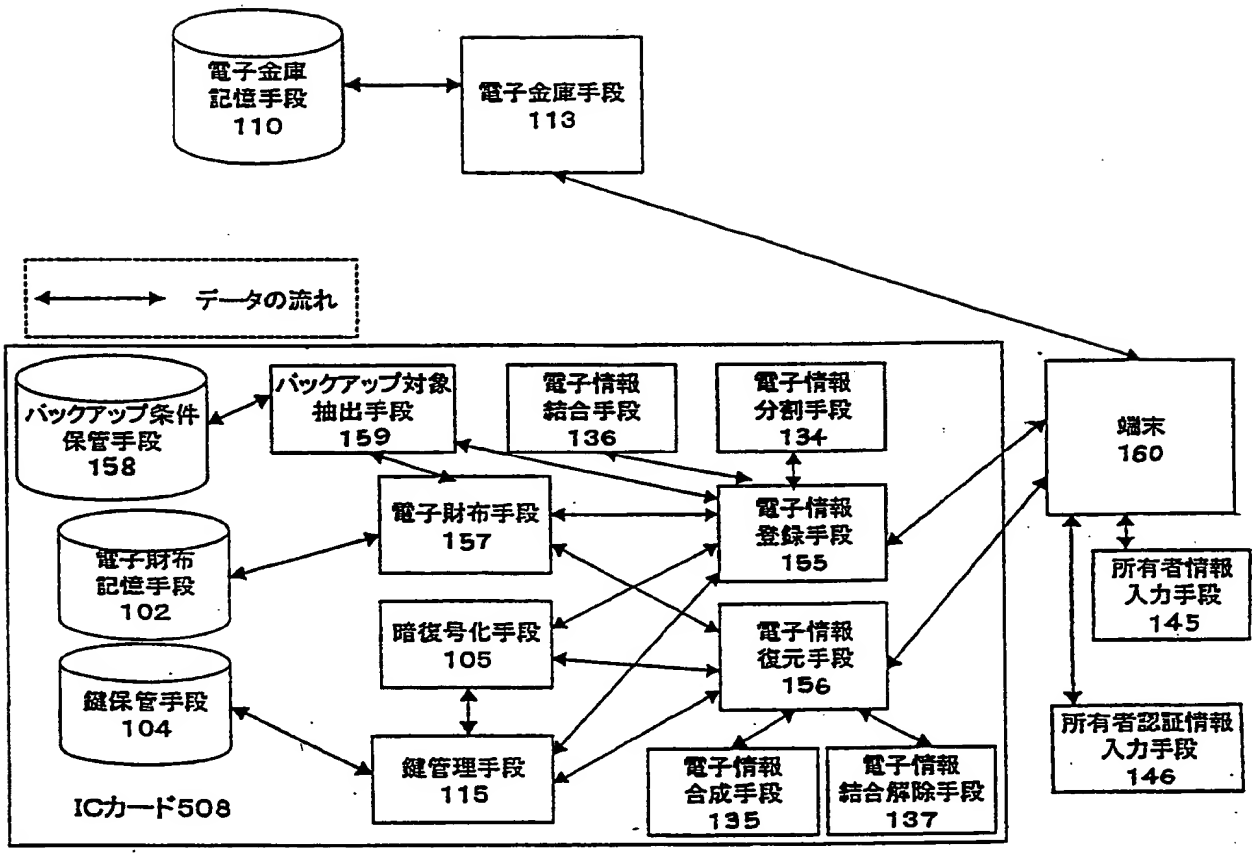

電子金庫
記憶手段
110
電子金庫手段
113
データの流れ
バックアップ条件
保管手段
158
バックアップ対象
抽出手段
159
電子情報
結合手段
136
電子情報
分割手段
134
端末
160
電子財布手段
157
電子情報
登録手段
155
電子財布
記憶手段
102
暗復号化手段
105
電子情報
復元手段
156
所有者情報
入力手段
145
鍵保管手段
104
鍵管理手段
115
電子情報
合成手段
135
電子情報
結合解除手段
137
所有者認証情報
入力手段
146
ICカード508

図19

情報種別	映画チケット	コンサートチケット	プリペイドカード	映画チケット
名前	A	C	E	G
単価	1600円	4500円	1000円	1600円
数	1	2	1	2
合計金額	1600円	9000円	1000円	3200円
場所	B	D	F	H
有効期間	2000年4月1日～2000年5月31日	2000年4月29日～2000年4月29日	無期限	2000年5月1日～2000年6月30日
残金	0円	0円	800円	0円

図20

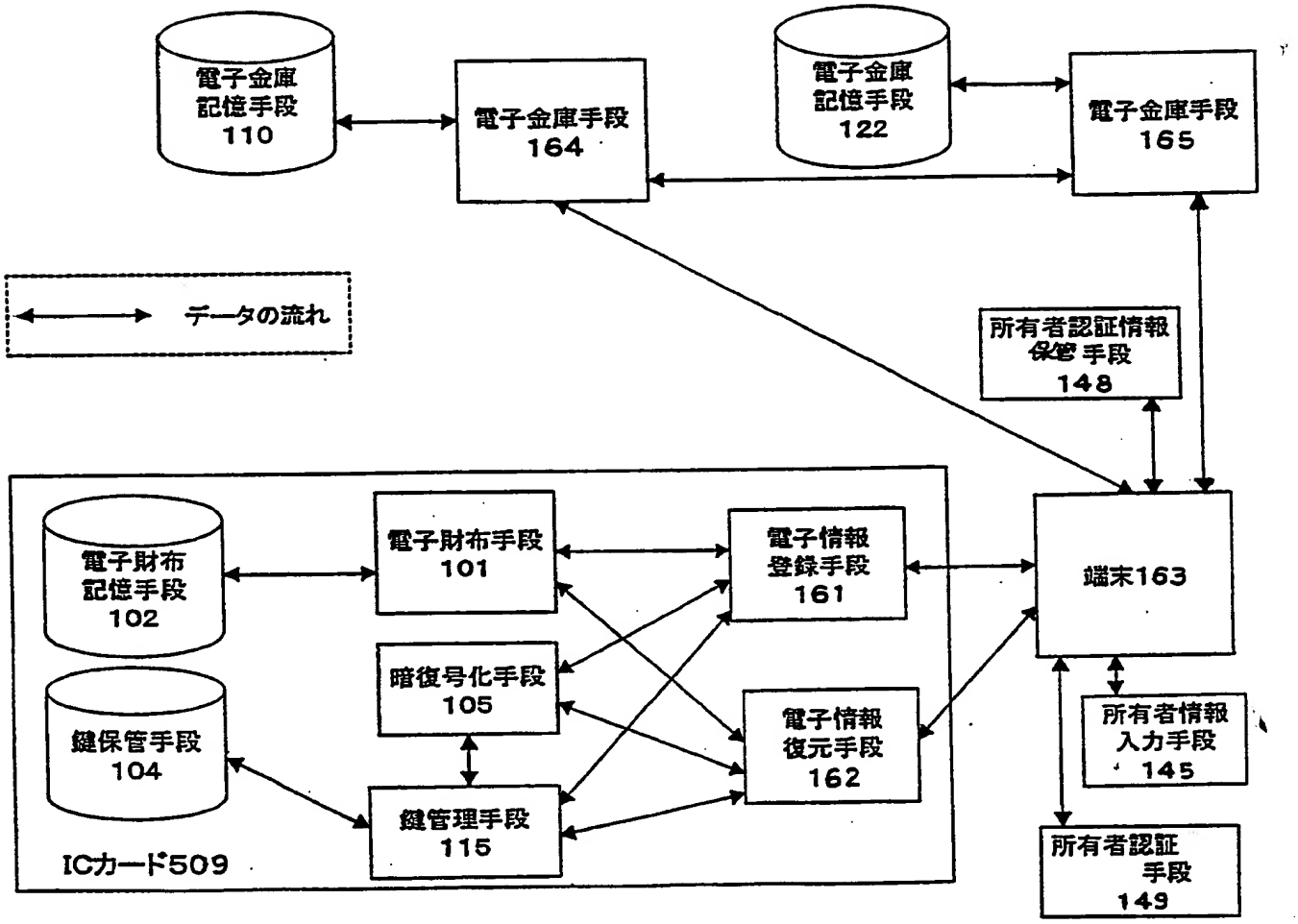
映画チケット	映画チケット
A	G
1600円	1600円
1	2
1600円	3200円
B	H
2000年4月1日～2000年5月31日	2000年5月1日～2000年6月30日
0円	0円

(a)

プリペイドカード	映画チケット
E	G
1000円	1600円
1	2
1000円	3200円
F	H
無期限	2000年5月1日～2000年6月30日
800円	0円

(b)

図21


電子金庫
記憶手段
110
電子金庫手段
164
電子金庫
記憶手段
122
電子金庫手段
165
データの流れ
所有者認証情報
保管手段
148
電子財布
記憶手段
102
電子財布手段
101
電子情報
登録手段
161
端末163
暗復号化手段
105
鍵保管手段
104
電子情報
復元手段
162
所有者情報
入力手段
145
鍵管理手段
115
所有者認証
手段
149
ICカード509

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05439

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F 17/60 G06F 19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/05673, A1 (Trusted Information Systems Inc), 22 February, 1996 (22.02.96) & AU, 33217/95, A & BR, 95/08548, A & CA, 2197206, A1 & CN, 1158195, A & EP, 775401, A1 & JP, 10-508438, A & US, 5991406, A & US, 5956403, A & US, 5745573, A & US, 5640454, A & US, 5557765, A & US, 5557346, A "3. Third Embodiment - Data Recovery Centers"	27-44
X	WO, 98/35472, A1 (Connected Corp), 13 August, 1998 (13.08.98) & AU, 64342/98, A & AU, 61515/98, A & AU, 61510/98, A & US, 5940507, A & WO, 98/035306, A1 & WO, 98/035285, A2, A3 Full text	27,29-32
A	JP, 9-160990, A (Hitachi, Ltd.), 20 June, 1997 (20.06.97) (Family: none) Par. No. [0023]	1-44

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 November, 2000 (07.11.00)	21 November, 2000 (21.11.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05439

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, 97/02539, A1 (Hitachi, Ltd.), 13 August, 1998 (13.08.98) & AU, 63180/96, A & US, 6039250, A & EP, 241526, A1, B1 Full text	1-44
A, P	STOREY, Veda C et al., "A Conceptual Investigation of the E-Commerce Industry", in Communications of the ACM, Vol. 43, No 7, July 2000 (07.00), pp. 117-123. See the last sentence of the first section.	1-44

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５４３９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl.[7]　G06F 17/60

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl.[7]　G06F 17/60　G06F 19/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－2000年
日本国実用新案登録公報　1996－2000年
日本国登録実用新案公報　1994－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WO, 96/05673, A1 (Trusted Information Systems Inc) 22. 2月. 1996 (22.02.96) & AU, 33217/95, A & BR, 95/08548, A & CA, 2197206, A1 & CN, 1158195, A & EP, 775401, A1 & JP, 10-508438, A & US, 5991406, A	27–44

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
07.11.00	21.11.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	阿波　進	5L	9168
	電話番号　０３－３５８１－１１０１　内線　３５６１		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	& US, 5956403, A & US, 5745573, A & US, 5640454, A & US, 5557765, A & US, 5557346, A *"3. Third Embodiment — Data Recovery Centers" を見よ.*	
X	WO, 98/35472, A1 (Connected Corp) 13. 8月. 1998 (13.08.98) & AU, 64342/98, A & AU, 61515/98, A & AU, 61510/98, A & US, 5940507, A & WO, 98/035306, A1 & WO, 98/035285, A2, A3 *文書全体を見よ.*	27, 29–32
A	JP, 9-160990, A (株式会社日立製作所) 20. 6月. 1997 (20.06.97) (ファミリーなし) *段落[0023]を見よ.*	1–44
A	WO, 97/02539, A1 (株式会社日立製作所) 13. 8月. 1998 (13.08.98) & ~~AU,~~ 63180/96, A & US, 6039250, A & EP, 241526, A1, B1 *文書全体を見よ.*	1–44
A, P	STOREY, Veda C *et al*, "A Conceptual Investigation of the E-Commerce Industry", in *Communications of the ACM*, Vol 43, No 7, July 2000 (07.00), pp 117–123. *最初のセクションの最後の文を見よ.*	1–44